

4.10 Risk Management (*Satisfies iCMM Process Area (PA) 13 criteria*)

4.10.1 Introduction

The objective of Risk Management is to provide a proper balance between risk and opportunity. It seeks to understand and avoid the potential cost, schedule, and performance/technical risks to a project, and to take a proactive and well-planned role in anticipating them and responding to them if they occur. Risk Management is equally at home in project management as well as System Engineering (SE) because both domains have a common view of seeking out opportunities to solve a problem or fulfill a need. Opportunity represents the potential for improving value in achieving a goal; risk represents the potential for decreasing the same value. Hence, any discussion of Risk Management is concomitant with the subject of opportunity management. The methodologies, decision parameters, and outcomes apply as well to risks as they do to opportunities.

The Risk Management process (Figure 4.10-1) provides an organized, systematic decision-making methodology to effectively deal with uncertainty in accomplishing program and/or organizational objectives. **Risk is defined as a future event or situation with a realistic (non-zero nor 100 percent) likelihood/probability of occurring and an unfavorable consequence/impact to the successful accomplishment of well-defined goals if it occurs.**



The PMBOK® Guide Chapter 11 Project Risk Management states that risks can have a positive or negative outcome. The approach outlined in this chapter recognizes risk as dealing with the negative side of the value proposition and recognizes that the positive side of the value chain is reserved to the management of opportunity.

Risk Management is an organized, systematic decision-support process that identifies risks, assesses or analyzes risks, and effectively mitigates or eliminates risks to achieve objectives. A risk creates an exposure to failure based on the combined effect of its likelihood and consequence, referred to as the “risk exposure”. Because the risk exposure can appear and be treated at various levels and stages of a program, the Risk Management process must be applied at all levels of activity. This means that the process is applied to small projects and large programs, across all aspects of a program or organization (see Figure 4.10-2), and continuously throughout the program's lifecycle. The extent and depth of application of this process should be governed by the outcome(s) being supported. In other words, what decisions are involved at a given point in the lifecycle, and what are the relevant risk factors to be addressed to support those decisions? The risks shall be managed in a way that they are capable of being “rolled up” from a project or several projects to a program. Risk rollup involves a review of the consequences/impacts from a higher (program or organizational) level. The risks to meeting the objectives or benefits of these projects or programs are typically known as programmatic risks, though the source of these risks may be external to the program itself. This process complies with the requirements of the integrated Capability Maturity Model (iCMM) (PA 13). It also satisfies Electronic Industries Alliance (EIA) 632 requirement 24 and EIA 731 Focus Areas 2.5-2 through 2.5-8.

For the purpose of this section, the terms “program,” “project,” and “organization” are used interchangeably, except where the context infers otherwise. In those instances, a program is generally viewed as consisting of related projects and is usually part of an organization.

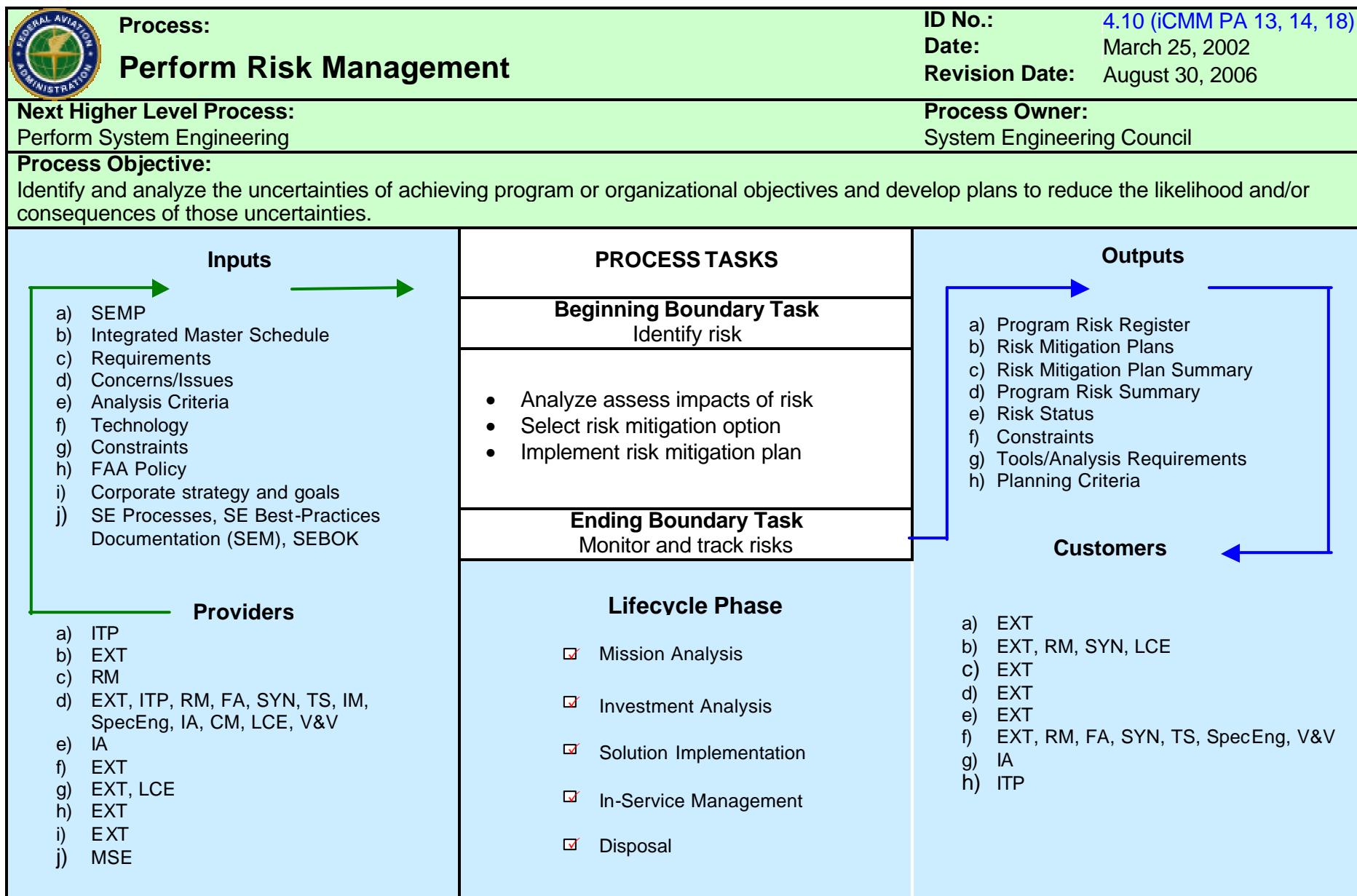
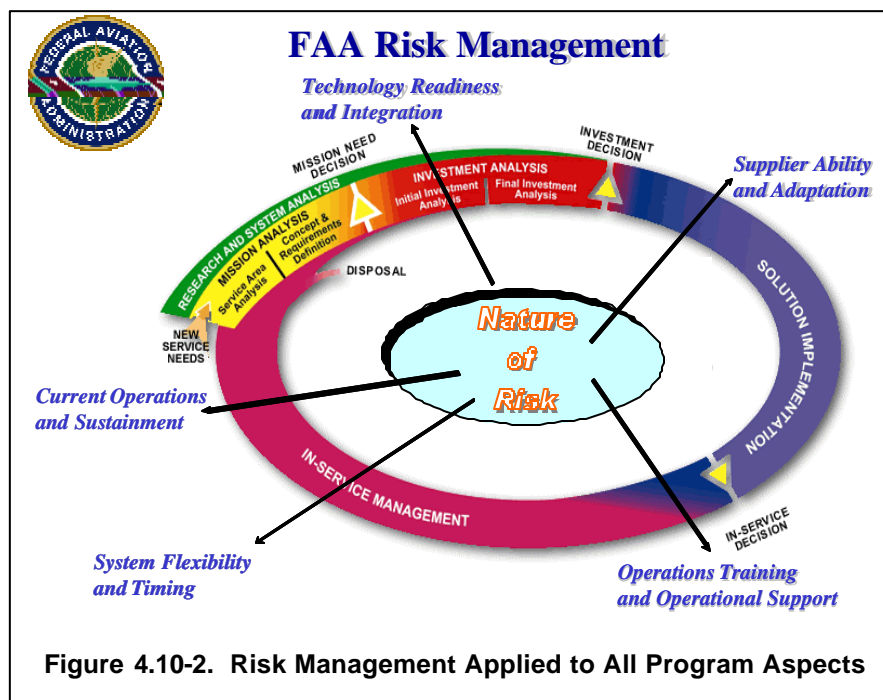


Figure 4.10-1. Risk Management Process-Based Management Chart



4.10.1.1 Function of Risk Management

Risk management is a basic SE element of successful program management (Figure 4.10-3). When properly executed, Risk Management engages all disciplines and execution teams and is present in all program stages and phases. The functions (Figure 4.10-4) of the process are to:

- Identify each risk to the program
- Analyze and assess the negative consequences/impact and the likelihood/probability of the risk actually occurring and determine the risk realization date
- Develop specific approaches and plans to mitigate the risk
- Implement the risk mitigation plan
- Monitor and track risk mitigation effectiveness

Based on results from these functions, program management may then determine:

- The schedule and budget reserves to be allocated and to what, based on identified risks
- How to measure overall program performance regarding each risk
- How much and what type of help is needed from other sources
- When to look at the process to see if the mitigation effort is working
- When to add mitigation efforts, costs, and milestones to the integrated program schedule and budget

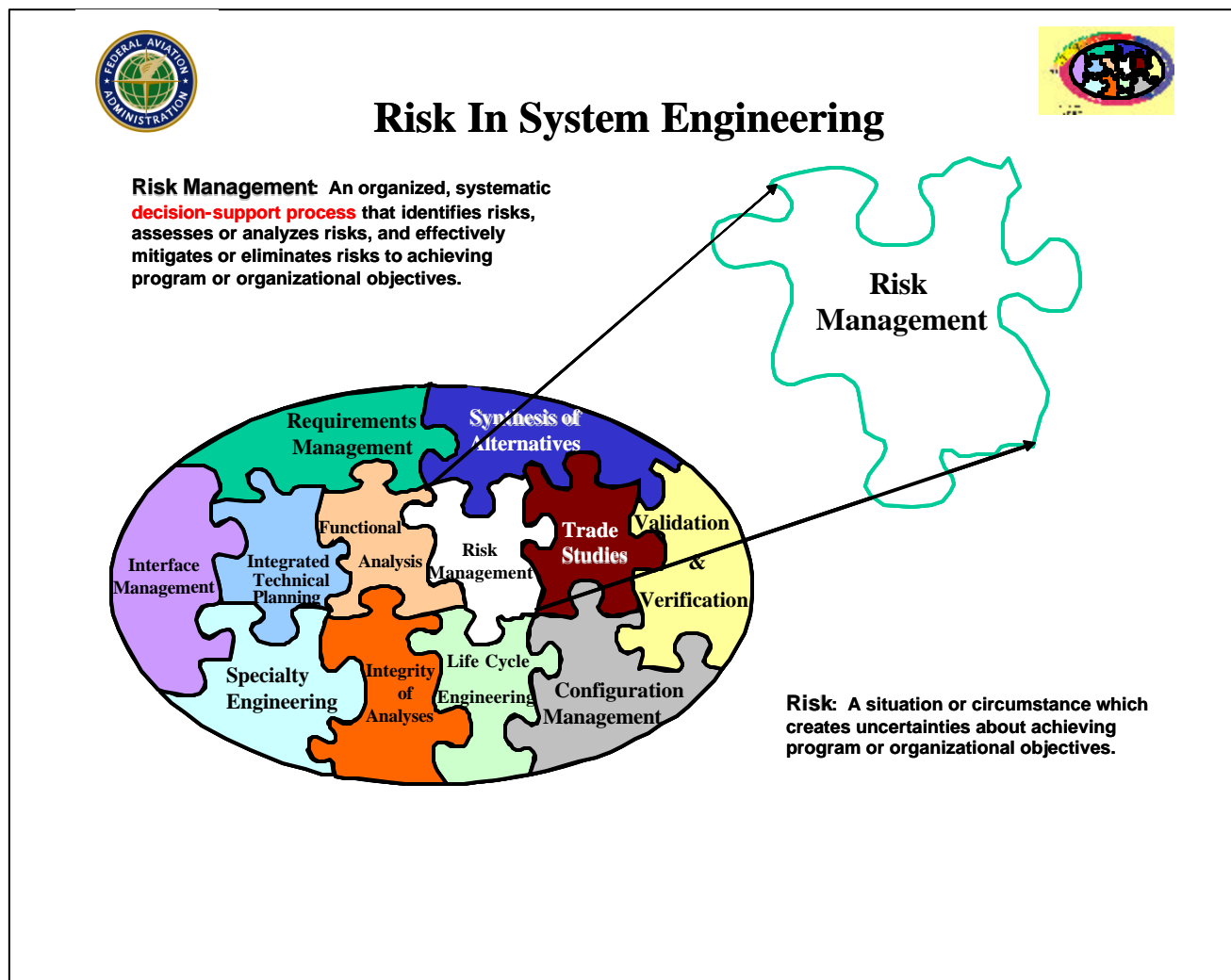


Figure 4.10-3. Risk in System Engineering

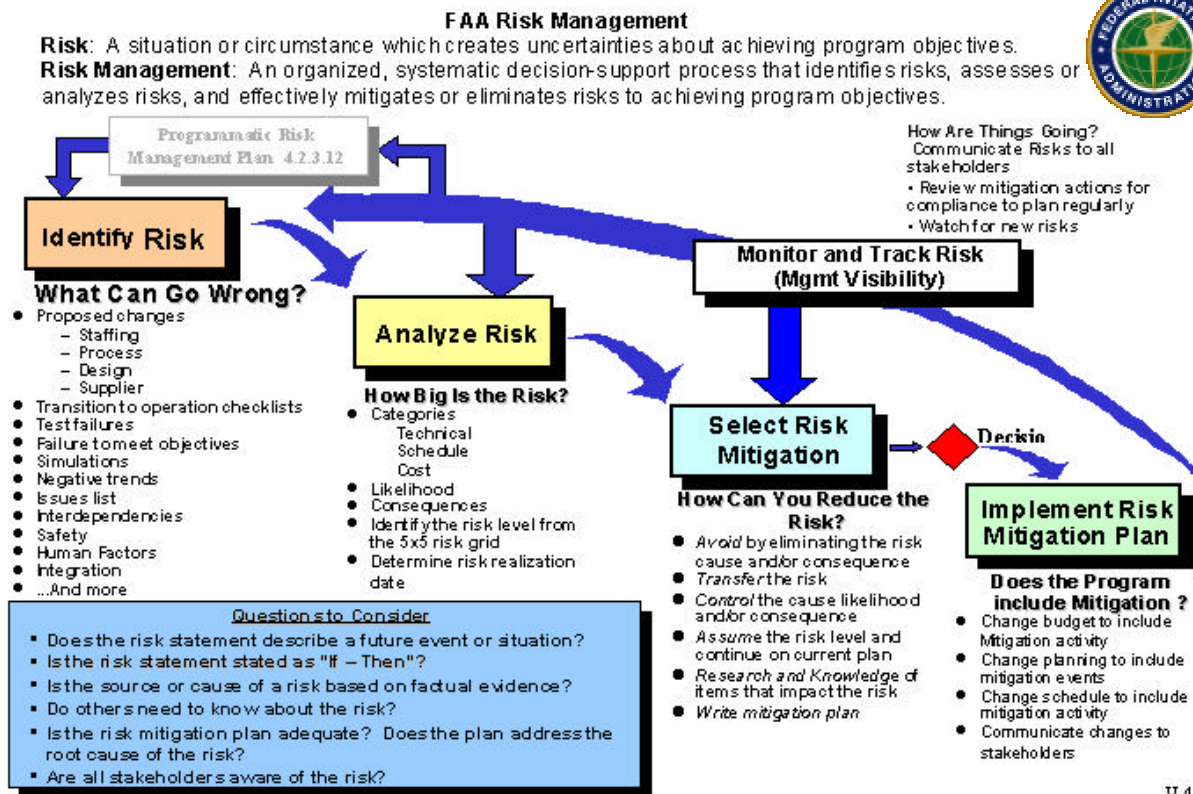


Figure 4.10-4. FAA Risk Management Process

4.10.1.2 Objectives of Risk Management

Within the opportunity-risk paradigm, the fundamental objective of the Risk Management process is to identify and analyze uncertainties of achieving program or organizational objectives and develop plans to reduce the likelihood and/or consequences of those uncertainties.

This process is applied to ensure that a program or organization meets technical, schedule, and cost commitments; delivers a product or service that satisfies all stakeholders' lifecycle needs; and provides the expected benefit. Four lower-level objectives are established as part of the overall objective:

- Timely identification of risks (identifying a potential problem with sufficient lead time so that the team may implement appropriate alternate plans)
- Consistent assessment of the level of risk across a program (providing a structured decision making framework for prioritizing resource application)
- Communication of risk mitigation actions across the program/organization (ensuring that all elements of the program/organization are aligned in resolving risks)
- Review of risk mitigation action performance

4.10.2 Process Description (*Satisfies iCMM PA-14, BP13.04 criteria*)

Every participant in a program/organization shares the responsibility of assessing and mitigating risks. The process is a part of the overall program/project management and system engineering process(es). This process shall be aligned with the individual products (hardware, services, and

software) that result from consistent functional analysis and requirements allocations, the System Engineering Management Plan (SEMP), the integrated program schedule, the associated funding, and the identified goals and benefits. The effort involved is assessed as to risks associated with impacts on benefits, interdependencies with other programs/organizations, or environments. For each product, risks are evaluated against the established operating baseline technical requirements, schedule, and cost leading to the successful satisfaction of the program/organizational objectives. Risks are identified, assessed, and appropriate risk mitigation actions established that comply with the governing risk management plan (see Section 4.2, Integrated Technical Planning). This plan is developed and tailored (when the nature of the effort demands tailoring per Section 3.5) to satisfy the specific program/organizational needs. (*Satisfies iCMM BP 13.01 criteria*)

Results from each assessment are a starting point for the risk mitigation plan to support management decisions (technical, schedule, and cost). The products of this process are also shared with stakeholders to achieve alignment/acceptance of the resource decisions. All risks are examined at each program/project/event/item/peer review as defined in the risk management plan. Updates reflect changes in risk resulting from planned mitigation activities or other unplanned events. Risk progress is actively tracked. For each risk, a "risk realization date" is established, marking the point in time when either the risk no longer exists or when the risk becomes a fact, and the program may have to be modified to accommodate the negative consequences. This point in time can be expressed as either an absolute (date, etc.) or in relative terms (project milestones, events, etc.). The question to be asked and answered is: "What happens at this point in time?" Risk is "rolled up" when it is taken from a lower-level project to a higher-level program or from a lower-level organization to a higher one for review and mitigation.

An essential element of the Federal Aviation Administration (FAA) Risk Management process from an organizational point of view is the non-advocate concept. The purpose of a non-advocate is to provide an impartial, objective assessment of the project team's results, especially regarding assignment of risk levels. The input of a non-advocate is essential on those projects where two or more of the project specialists disagree on the risk levels. A non-advocate would typically be, but not limited to, a program management person (above or at the same level of the program/project manager); a stakeholder representative; and/or a person from another project or program. The responsibility of a non-advocate is to examine and assess all aspects of the program/project risk management process before each review. For small projects, one or two non-advocates may be acceptable. A non-advocate provides an assessment to program/project managers for consideration and action.

4.10.2.1 Overview

Figure 4.10-1 shows the top-level process for Risk Management. The process includes steps that result in identification of potential risks, analysis and assessment of risk, development of risk mitigation plans, implementation of the Risk Mitigation Plan, and monitoring of risk status. The process is iterative and is used across the program throughout the program's lifecycle, with the nature of the risks changing to coincide with the lifecycle stage. Table 4.10-1 illustrates the

Table 4.10-1. Risk Management and the AMS Lifecycle Phases

Risk Activity	R&D to Mission Analysis	Initial Investment Analysis	Final Investment Analysis	Beyond Investment Analysis
Risk Focus	Assessment of operational risk associated with new concepts	Assessment of comparative risks between alternatives	Lifecycle risks of the selected alternative; Risk Management Plan updated for Implementation	Program execution Acquisition and/or Program Reviews
Depth of Risk Assessment	High-level	Some detail	More detailed	Detailed
Risk Products	Identification of potential risks General risks and requirements for any proposed alternative	Comparative risk analysis for each alternative Initial risk-adjusted cost and benefits baseline	Updated Risk Analysis Risk Management Plan (in SEMP) Final risk-adjusted cost and benefits Baseline	Risk Management Plan Risk Tracking Matrix Etc.
Risk Leadership Role	Stakeholder/Organization	Investment Analysis Team	Investment Analysis Team	Program/Sponsor/System Operator

lifecycle dimension of Risk Management. Specific knowledge domains implement variants of this process to fit their specific needs and environment. However, all domains effectively perform Risk Management, as shown in Figure 4.10-4.

4.10.2.2 Inputs

An expanded set of inputs capable of initiating Risk Management includes both program/project and product-related data as shown in Table 4.10-2. Many of these inputs are developed and refined through the continuous, iterative use of other system engineering processes. Each table item is to be evaluated for resultant program risk. (Items in bold appear in Figure 4.10-1 Process-Based Management Chart.)

Table 4.10-2. Inputs to Risk Management

Input	Reference
Risk Mgmt Plan	4.2.1
System Engineering Management Plan (SEMP)	4.2.3.2
Integrated Safety Plan	4.2
Implementation Strategy and Planning	4.2
Test plans	4.12
Integrated Program Schedule	4.2
Requirements	4.3.3
Mission Need and Concepts	4.4
Interfaces	4.7
Statement of Work	4.3
Issues/Concerns	Appendix D
Trade Study Results	4.6.1.4
Design Analysis Results	4.8.4.3
Controlled Data and Reports	4.11.8
Specialty Engineering Analysis Results	4.8
Safety and/or Security Assessments	4.8
Human Factors Assessments	4.8
Verification Results	4.12
Training Results	4.14
Maintenance Results	4.13
Operational Results	4.13
Lessons Learned	4.14
Program Review Results	4.2.6
Analysis Criteria	4.9.5.5
External Environmental Forces	
ISAP (Internal Exhibit 300)	FAST
System Engineering Reviews	4.2.6
Contractor Outputs	
Technology	
Constraints	
Enterprise Architecture (EA)	4.5.5
Manufacturing/Production Information	4.5
Product Configuration Data	4.11.3
Resources/Budgets	
FAA Policy	
AMS Documents	FAST
Corporate Strategy and Goals	
Contract	

4.10.3 Risk Management Process Tasks

Figure 4.10-1 summarizes the Risk Management process. The remainder of this section describes the major process steps, as shown in Figure 4.10-4.

4.10.3.1 Task 1: Identify Risk (*Satisfies iCMM BP 13.02 criteria*)

Risk identification is a systematic effort to uncover possible events or conditions that, if they occur, may hinder achievement of program or organization objectives. The process begins concurrently with program or project planning and continues throughout the life of the program. In each instance, the question to be asked is: "What can go wrong or interfere with success?" While risk events or conditions may have many different root causes (e.g., equipment interoperability requirements, maintainability and supportability requirements, installation deadlines, contractual arrangements), the identification process isolates those events or conditions that may affect program technical performance, cost performance, or the program schedule. At the conclusion of the identification phase of risk management, it is recommended that a program manager have a list of (uncertain) events and conditions that may affect program cost, schedule, and/or technical performance. Risk identification shall be performed during each stage of the program, or whenever significant changes occur in plans or program status. Circumstances requiring assessment for potential risks include:

- Programmatic changes (including schedules and cost milestones)
- Unfavorable trends in Technical Performance Measures, predicted system performance, schedules, and financial status
- Design/program/peer reviews
- Change proposals (including proposed changes in requirements)
- Occurrence of a major unforeseen event
- Newly identified risks
- Special assessments at the direction of agency management
- Changes or risks in interdependent programs
- Environment changes

As shown in Figure 4.10-5, participants in risk identification include all stakeholders, users, suppliers, and execution teams. Teams consider all likely risk sources in identifying potential risks to the program/project. Risk identification is based on the current program/project goals supported by the associated technical, schedule, and cost requirements and plans.



A risk has three aspects: (1) the event is in the future, (2) the likelihood/probability that an event will occur (a degree of uncertainty), and (3) a negative or unfavorable consequence/impact if it occurs. It is recommended that the likelihood of a risk occurring not be

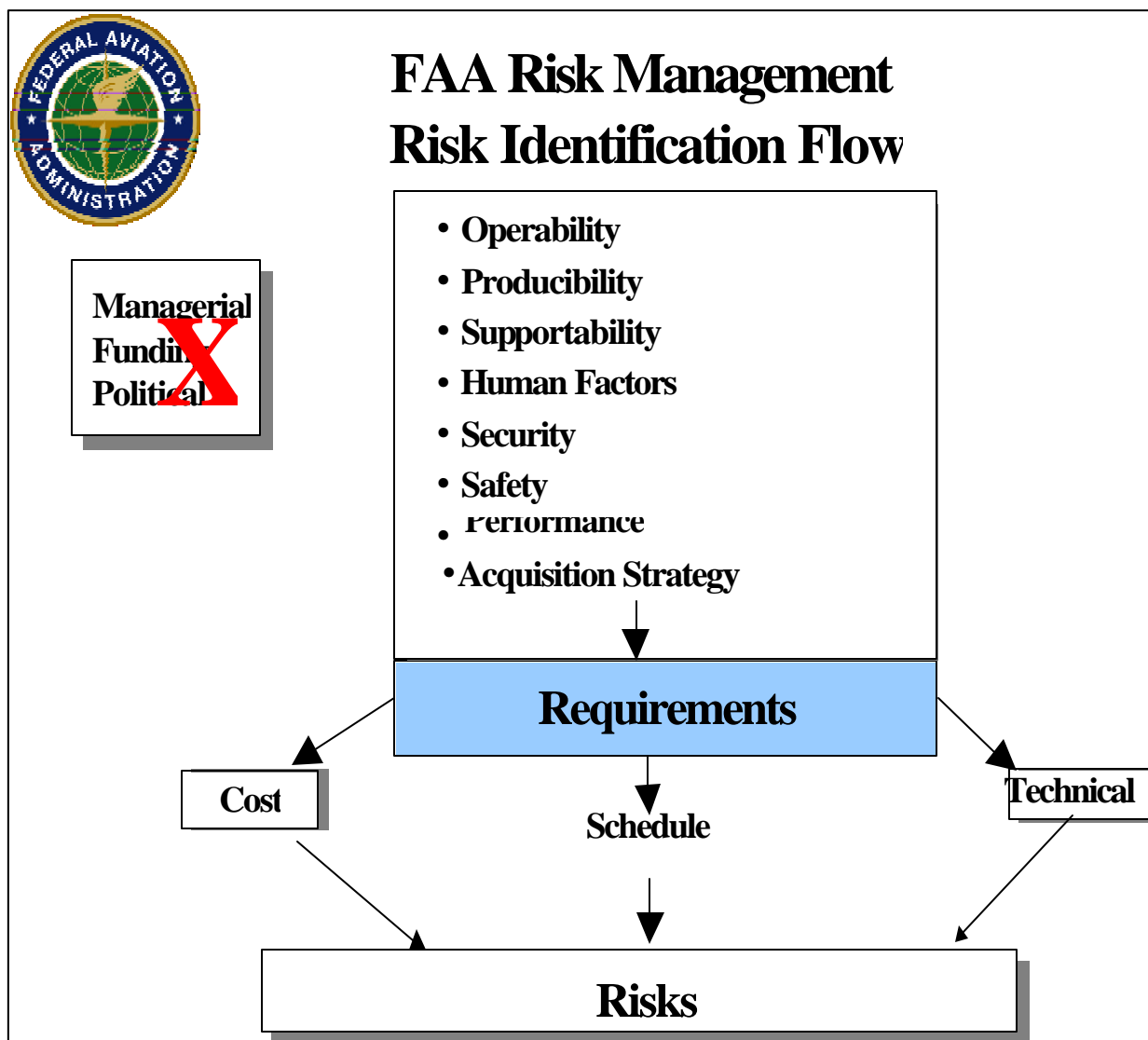


Figure 4.10-5. Risk Identification Flow

so low as to be negligible (i.e., probability essentially equal to zero) nor be equal to 1, which typically indicates that it has, in fact, already been realized. A risk shall also have a negative consequence/impact if realized. If ANY of these three characteristics are missing, the situation under consideration is handled as either an issue or a concern.

Positive variances to plan or consequences are not considered in the FAA risk identification and analysis process; these are considered opportunities. Note that if **ANY** of these three aspects are missing (i.e., the situation or circumstance is certain to occur or has already occurred), there is no risk, even though the item has an unfavorable consequence. It is recommended that this situation be handled as a management issue or concern, for which a corrective action plan shall be generated and implemented.

As discussed in subsection 4.10.2 above, each risk has a “risk realization date”. The negative consequence of the outcome of the event that occurs on a given date is the basis for the risk. It is very important to identify and document this point in time as early as possible to ensure that only active risks consume the organization’s attention and resources.

4.10.3.1.1 Potential Sources of Risk

Risks originate from three basic areas—technical (or performance), schedule, and cost. The determination of which area or category a risk falls into is determined by its root cause. Figure 4.10-5 shows a risk identification flow. Technical risk is based on the likelihood that the program as planned will be unable to deliver a product or service to satisfy the technical requirements. As such, well-documented, defined, and quantified technical requirements are necessary to define a technical risk. Schedule risk results from the likelihood that the program actions may not be accomplished in the planned program timing. A detailed program schedule identifying each accomplishment and the critical path is necessary to develop schedule risks. Cost risk results from the likelihood that the program may not accomplish planned tasks within the planned budget. A detailed budget, in which the cost of each accomplishment is specified and any management reserve is known, is needed to determine a cost risk. Potential loss of funding is typically not a program risk because the funding decision is made at the Agency level, and the financial risk to the program occurs once a decision has been made to allocate the existing Agency funding among programs and/or organizations. Within the FAA risk process, *cost* is the expenditure required for a resource and the end product produced by that resource. *Budget* is the forecast of all costs planned for a given project/program, and *funding* is the supply of money provided to accomplish a given project/program. The risk source is based on the **root cause** of the risk and, as such, only a single source will cause a risk. The source is either technical, schedule, or cost in nature and not a combination or all of these. This is not to be confused with the symptoms, which may manifest themselves as some combination of performance (technical), benefit, cost, and/or schedule impact.

A program's acquisition strategy generates risks in its own right. Development programs using proprietary or custom designs are different in nature from those using commercial-off-the-shelf (COTS) solutions. Risks that need to be considered in a COTS-based acquisition appear in Figure 4-10.6.

Many sources must be considered for each risk area. For technical risk, likely sources include technology maturity, complexity, dependency, stakeholder uncertainty, requirements uncertainty, and testing/verification failure. Sources of schedule risks may include incomplete identification of tasks, time-based schedule (as opposed to event-based schedule), critical-path scheduling anomalies, competitive optimism, unrealistic requirements, and material availability shortfalls. Cost risks may stem from an uncertain number of production units, supplier optimism, additional complexity, change in economic conditions, competitive environment, supplier viability, and lack of applicable historical data.



Table 4.10-3 provides the potential sources of risk that shall be considered in the process of program risk assessment. This listing provides an excellent starting point for identifying potential risk areas when combined with the input factors appearing in Table 4.10-1, Risk Management and the AMS Lifecycle Phases.

Table 4.10-3. Potential Sources of Risk

Program Aspect	Common Risk Areas
Architecture	<ul style="list-style-type: none"> • System requirements flow-down not well defined. • Trade-off studies not performed early enough in the program to support system design with the best alternative. • Modeling and simulation use limited in more fully developing and evaluating potential architectures. • Functional interfaces between architecture elements not well defined.
Capability of Developer	<ul style="list-style-type: none"> • Developer has limited experience in specific type of development. • Contractor has poor track record relative to costs and schedule. • Contractor experiences loss of key personnel. • Contractor has poor track record relative to appropriate training for personnel. • Prime contractor relies excessively on subcontractors for major development
Concurrency	<ul style="list-style-type: none"> • Immature or unproven technologies will not be adequately developed before production. • Production funding will be available too early, before development effort has sufficiently matured.
Contracting	<ul style="list-style-type: none"> • Acquisition strategy unstable or changing; untimely acquisition strategy approval. • Key program documentation (specifications, interface documents) unavailable to support RFP package release. • Overall program definition (program strategy) unclear; cannot be clearly defined in program Statement of Objectives (SOO) for definition to the contractor. • Request for Proposal (RFP) package release schedule does not support overall program schedule needs. • Realistic cost objectives not established early. • Marginal technical capabilities incorporated at excessive costs.
Cost/Funding	<ul style="list-style-type: none"> • Satisfactory cost- technical tradeoffs not done. • Excessive life cycle costs due to inadequate treatment of support requirements. • Significant reliance on software.

Program Aspect	Common Risk Areas
Design	<ul style="list-style-type: none"> • Design implications not sufficiently considered prior to investment decision. • System will not satisfy user requirements. • Mismatch of user manpower or skill profiles with system design solution or human-machine interface problems. • Increased skills or more training requirements identified late in the acquisition process. • Design not cost effective. • Design relies on immature technologies or “exotic” materials to achieve technical objectives.
Integration	<ul style="list-style-type: none"> • Interface documentation is inadequate or not defined. • End to end performance has not been addressed. • System integration with legacy configurations is unclear.
Lifecycle	<ul style="list-style-type: none"> • Inadequate supportability late in development or after fielding, resulting in need for engineering changes, increased costs, and/or schedule delays. • Lifecycle costs not accurate because of poor logistics supportability analyses. • Logistics analyses results not included in cost-performance tradeoffs.
Management	<ul style="list-style-type: none"> • Acquisition strategy does not give adequate consideration to various essential elements (as mission need, operations, test and evaluation, technology). • Subordinate strategies and plans are not developed in a timely manner or based on the acquisition strategy. • Proper mix (experience, skills, stability) of people not assigned • Effective risk assessments not performed or results not understood and acted
Production/ Facilities	<ul style="list-style-type: none"> • Production implications not considered prior to investment decision. • Production not sufficiently considered during design. • Inadequate planning for long lead items and vendor support. • Production processes not proven. • Prime contractors do not have adequate plans for managing subcontractors. • Operational requirements not properly established or vaguely stated. • Requirements are not stable.
Requirement Set	<ul style="list-style-type: none"> • Required operating environment not described. • Requirements do not address logistics and suitability. • Requirements are too constrictive—identify specific solutions that force high cost. • Requirements are not verifiable.

Program Aspect	Common Risk Areas
Safety	<ul style="list-style-type: none"> • Safety management program not established early in the life cycle. • Program and subject matter expert coordination is limited with safety professionals. • Safety analysis assumptions inadequate or not defined. • Safety analyses not performed on changes.
Schedule	<ul style="list-style-type: none"> • Schedule not considered in trade-off studies. • Schedule does not reflect realistic acquisition planning. • Schedule objectives not realistic and attainable. • Resources not available to meet schedule. • System security requirements not specified sufficiently or timely enough to support system design needs.
Security	<ul style="list-style-type: none"> • System security interface definition (cryptography, keys, fill devices, message structure) with the individual program elements is unclear or immature. • Limited program involvement and coordination with system security developers and providers (NSA for example). • Security implications not adequately considered in architecture. • Uncertainty in threat accuracy.
Simulation	<ul style="list-style-type: none"> • Tools and reference models are not validated. • Maintenance and Support are not verified, validated, or accredited for the intended purpose. • Program lacks proper tools and modeling and simulation capability to assess • Program depends on unproved technology for success—there are no alternatives.
Technology	<ul style="list-style-type: none"> • Program success depends on achieving advances in state-of-the-art technology. • Potential advances in technology will result in less than optimal cost-effective system or make system components obsolete. • Technology has not been demonstrated in required operating environment.
Test and Evaluation	<ul style="list-style-type: none"> • Test planning is not initiated early in program. • Testing does not address the ultimate operating environment. • Test procedures do not address all major technical and suitability requirements. • Test facilities not available to accomplish specific tests, especially system-level tests. • Insufficient time allowed in the schedule to test thoroughly.

COTS Considerations

<i>Number</i>	<i>COTS Risk Factor (Characteristic)</i>
01	COTS products can exhibit rapid and asynchronous changes.
02	COTS product obsolescence can affect systems in different ways.
03	COTS products are typically documented with proprietary data.
04	Low initial costs of COTS products can be offset by higher lifecycle costs.
05	Functionally equivalent COTS products/systems can have multiple configurations.
06	Different COTS product vendors have different quality practices.
07	COTS products form, fit, and function are sold “as is.”
08	COTS products are developed to commercial standards.
09	COTS products typically have time-limited manufacturer support.
10	COTS product interoperability can introduce information security susceptibility.

Figure 4.10-6. COTS-Based Risk Considerations

The knowledge domains of safety and security impose additional criteria or gates as part of their identification process. In the case of safety, the process commences with an analysis, which identifies potential hazards that are the basis for identifying safety-related risks. Safety does not identify a risk until a hazardous situation has been identified.

Information security engineering also utilizes a series of gates prior to identifying a risk. Security is concerned about the existence of viable threats, which may exploit a system vulnerability to cause harm. The combination of a viable threat coupled with a vulnerability in the system that is capable of being exploited by the threat is necessary before the security community moves to declare a (security) risk.

4.10.3.1.2 Risk Identification Methods

Risk identification begins at the lowest feasible level and normally includes inputs from all stakeholders and suppliers. Anyone may identify a potential risk. The objective of this step is to produce a list of potential risks that is as comprehensive as possible. It is recommended that the focus be on root causes and not on symptoms of a more basic problem. The problem shall be defined at the lowest level (root cause) so that the mitigation plan actually addresses the problem. It is recommended that experts review previous programs to determine that risks related to their domain(s) have been completely identified. It is also recommended that similar programs be reviewed for determined risks as well as actual problems. This may be achieved using any combination of methods, such as group discussions, interviews, trend/failure analysis, risk templates, lessons learned, trade studies, best practices, metrics, and acquisition documentation.

This process includes a final step to validate or screen the list of proposed risks prior to committing them to the risk repository or database. This validation should ensure that the risks identified are germane to the effort at hand and look for duplication and consolidation as appropriate. A “risk owner” should be assigned to each validated risk in accordance with the provisions of the Risk Management Plan (RMP) to manage the efforts associated with and be responsible for that risk as it progresses through its own lifecycle. Once the proposed risk has been entered into the organization’s master risk database, it has effectively been approved by management as warranting further effort to address. The extent of that effort is governed by the provisions of the RMP.

Program Management errors are not risks and shall be corrected before the program moves forward. It is recommended that this screening consider program-level ramifications and ensure that program integration risks are adequately covered.



A Risk Worksheet (Figure 4.10-7) may be used to document newly identified potential risks and provide a documented trail of actions taken to determine the plan to reduce a given risk to an acceptable level.

4.10.3.1.3 Risk Statements

Risk statements frame the problem space. The investment made in properly structuring the risk statement is inversely proportional to the effort expended to deal with the risk. If little to no effort is expended upfront, then a disproportionate amount can be spent “chasing” the wrong problem. A rule of thumb for identifying risks is to state each risk candidate in “condition ... if ... then ...” format. If a certain event occurs, then there will be a certain consequence. Using this form makes it is easy to determine the validity of a risk. This construct generates a “strong” risk statement.

If the statement does not make sense or cannot be put in this format, then the candidate is probably not a true risk, and the resulting statement is considered weak. For example, a statement that has the “if” element but not the “then” implies that the potential event will not affect the project. Similarly, a statement with the “then” element but not the “if” implies there is an issue that will certainly affect the project, but no uncertainty about its occurrence. Table 4.10-4 contains some examples of weak risk statements gleaned from recent FAA Exhibit 300s prepared for submittal to the Office of Management and Budget (OMB). Each example has one or more essential elements missing to define the problem space and provide a solid basis for actions taken to deal with the (perceived) risk.

Table 4.10-4. Weak Risk Statements

If COTS components become technically obsolete before planned, the system could be difficult to maintain, maintenance costs could rise, or tech refresh could be required sooner than planned.
(Deployed) systems could become inoperative due to hardware and or COTS obsolescence.
Investment fails to deliver promised capability to field sites due to failure to take holistic view of effort.
Instability in the market place may lead to a supplier being unable to continue (to participate) in (this program).
Internal and external risks for (the system) gathering weather data and processing it into usable

and accurate weather information. <i>(Note: This is reviewed on an Annual basis. July 2004)</i>
(There may be) sudden or critical reductions in key project resources that can hinder the normal (project) processes. <i>(Note: This is reviewed on a weekly basis. 02/15/05)</i>
Technology (being used) not adequate for future requirements and expansion.
The government does not have experienced personnel for the management and acquisition of this investment.



A strong risk statement includes descriptions of the future event or condition, which confirms a potential problem; the root cause(s) of the event outcome or conditions; and the specific negative consequences to the program if the event or conditions occur. Subsection 4.10.3.2.3 discusses the methodology to determine the relative import of a risk. The construct of a strong risk statement provides a powerful means to accomplish that task. Table 4.10-5 illustrates the characteristics of strong a risk statement extracted from examples in recent FAA Exhibit 300s prepared for submittal to OMB (details have been changed for illustrative purposes).

Table 4.10-5. The Anatomy of a Strong Risk Statement

(Risk #216) If either the multiple SMR SAT completion or the start of the ASDE-X Safety Logic Optimization by July 15, 2006 is delayed in any way, then the commissioning of the new Atlanta ATCT and the IOC date of May 1, 2007 will be delayed, which will not meet the terms of the AT/NATCA MOU.
(Risk #305) If the Safety logic design and associated performance does not meet the operational expectations at Orlando International (MCO), then the ability to achieve ISD and deploy at other sites per the deployment schedule will be at risk with continued potential of accidents caused by runway incursion incidents at those locations.
(Risk # 389) If adjustments are not made to the installation schedule to accommodate aggressive intervals for key activities, the ASDE-X system may be in jeopardy to meet the Operational Required Date at Seattle International ... in time to support the decommissioning of ASDE-3 in August 2007, as required in the MOU with the Port of Seattle.

4.10.3.2 Task 2: Analyze and Assess Impacts of Risk (*Satisfies iCMM BP 13.03 criteria*)

Risk analysis or risk assessment provides program insight into the significance of identified risks. Risk analysis attempts to assess the likelihood of identified risks and the consequence to the program/organization if the risk event or condition occurs. The process also classifies each risk according to the root cause of the risk event (cost, schedule, or technical performance).



FAA Risk Worksheet

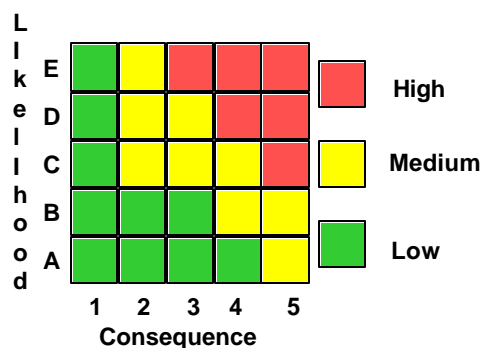
Program/Project Title _____ Seq. #: _____

Submitted by: _____ Date: _____

Risk:	Point of Contact
-------	------------------

Source and Root Cause:

<table border="1" style="width: 100%;"> <tr> <th colspan="4">Risk Assessment</th> </tr> <tr> <td><input type="checkbox"/> Technical</td> <td><input type="checkbox"/> Schedule</td> <td colspan="2"><input type="checkbox"/> Cost</td> </tr> <tr> <td>Likelihood</td> <td colspan="3">A B C D E</td> </tr> <tr> <td>Consequence</td> <td colspan="3">1 2 3 4 5</td> </tr> </table>	Risk Assessment				<input type="checkbox"/> Technical	<input type="checkbox"/> Schedule	<input type="checkbox"/> Cost		Likelihood	A B C D E			Consequence	1 2 3 4 5			Rationale
Risk Assessment																	
<input type="checkbox"/> Technical	<input type="checkbox"/> Schedule	<input type="checkbox"/> Cost															
Likelihood	A B C D E																
Consequence	1 2 3 4 5																



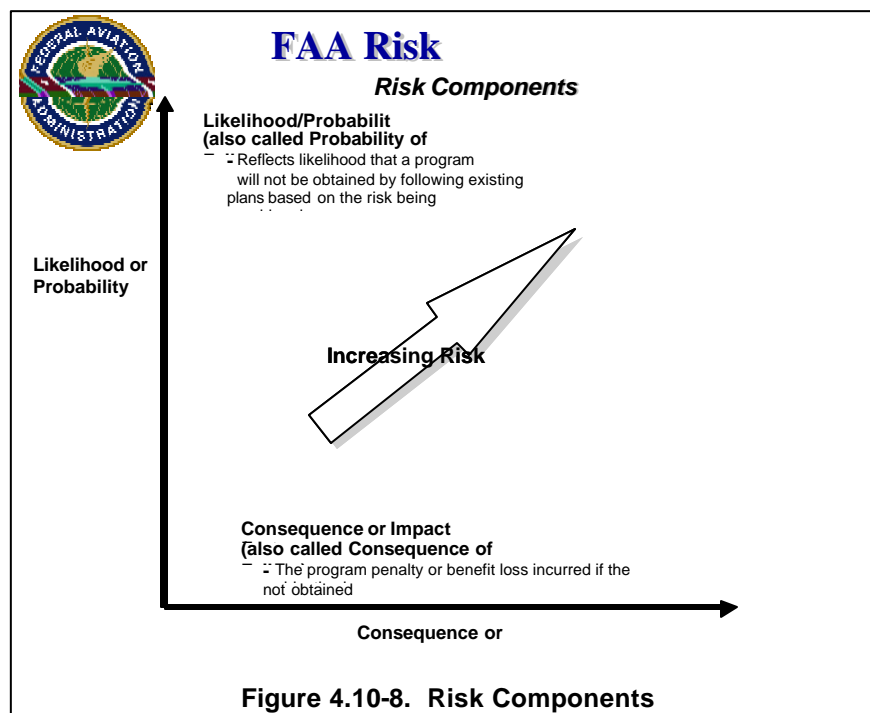
Consequence Definition:

	Risk Realization Date:
--	------------------------

5	Mitigation Options	Description	New Risk Level if Implemented
<input type="checkbox"/>	Avoidance		H M L
<input type="checkbox"/>	Transfer		H M L
<input type="checkbox"/>	Control		H M L
<input type="checkbox"/>	Assumption		H M L
<input type="checkbox"/>	Research & Knowledge		H M L

Submitted: _____	Date: _____	<input type="checkbox"/> Mitigation Approved	<input type="checkbox"/> Disapproved
Approval: _____	Date: _____	<input type="checkbox"/> Approved w/ Change	<input type="checkbox"/> Returned
		<input type="checkbox"/> Risk Accepted	<input type="checkbox"/> Closed

Figure 4.10-7. Risk Worksheet



Risk analysis assesses each of the two components of an identified risk — (1) the likelihood of the risk occurring, and (2) the consequence to the program if it occurs — as depicted in Figure 4.10-8. The basic tool used for qualitative risk analysis is the risk template, which contains a set of definitions to be used to evaluate the likelihood and consequence of a particular risk. The set of templates that a program uses may change over time as new templates are added or existing templates are changed, combined, or eliminated. The program may choose to use program-unique templates, which are based on and traceable to program or stakeholder requirements, provided supporting rationale is given. However, modification of templates limits the ability to “roll up” risks to a higher program level, and, as such, a mechanism shall be developed to correlate risks developed through modified templates to the risks developed with the standard FAA templates. The program/project is responsible for the choice, coordination, and control of the templates used on the program. These decisions are contained in the Risk Management planning section of the SEMP (see Section 4.2, Integrated Technical Planning of this document).

The result of the risk analysis process is assignment of a measure termed “risk exposure” to each identified risk. Risk exposure is one quantitative figure of merit that represents the combined effects of likelihood and consequence; it aids program management in ranking identified risks from most severe to least severe. At the conclusion of the risk analysis process, it is recommended that program management have visibility into the range of possible outcomes for the program (in terms of achieving objectives) if in fact an identified risk event or condition occurs.

4.10.3.2.1 Likelihood (Probability) Determination

A likelihood (probability) template is developed that applies to the specific risk/program under analysis. A new template is developed and documented if none of the existing program templates are applicable. This action shall be coordinated within the program/project and with higher levels of the organization using the criteria of the RMP. Correlation of the new templates

to the standard FAA templates in this manual shall be established. Figure 4.10-9 provides the FAA definitions of the risk likelihood levels.

4.10.3.2.2 Consequence Determinations

Another set of templates is used to evaluate consequence/impact to the program if the risk materializes. Consequences are ideally expressed in terms of dollars, specifically the cost of loss or recovery from that loss. Because of the difficulty of determining the costs in advance, templates are used to categorize the risks into relative groups of impact. Consequence templates are shown for three areas of program impact: technical (Figure 4.10-10), schedule (Figure 4.10-11), and cost (Figure 4.10-12). The choice of the consequence template to be used to evaluate a given risk is determined by the nature of the root cause of that risk. If the root cause is technical in nature, then the technical consequences template is used. It should be remembered that each of these templates results in a risk that threatens the benefits of a program and may also have interdependency impacts. The symptoms of the risk may materialize in any combination of program areas: technical (or performance), schedule, and/or cost. However, treating only the symptoms wastes program resources and does **NOT** directly deal with the source or root cause of the risk.

All NAS programs are developed to provide benefit(s) to the system. Risk ultimately reflects in impacts to benefit(s). All benefit losses are derived from negative impacts in either technical, schedule, or cost risks. This is a significant part of the risk consequence that must be defined. The cost/benefit analysis should be reexamined as a result of risk-driven impacts to provide the information needed to make informed decisions. As was the case with the likelihood templates, if none of the existing program consequence templates are applicable to a particular risk, new templates may be developed and documented. Correlation of the new templates to the standard FAA templates in this manual shall be established.



FAA Risk Likelihood Definitions

What is the likelihood the risk will happen?

- A. **Not Likely:** Your approach and processes will effectively avoid or mitigate this risk based on standard practices (<10% chance it **WILL** occur).

The chance of a negative outcome based on existing plans is not likely. This likelihood level assessment should be based on evidence or previous experience and not on subjective confidence. This assessment level requires the approach and processes to be well understood and documented. Little or no management oversight will be required.

- B. **Low:** Your approach and processes have usually mitigated this type of risk with minimal oversight in similar cases (<1/3 chance that it **WILL** occur).

There is a low likelihood but reasonable probability that a negative outcome is possible. Present plans include adequate margins (technical, schedule, or cost) to handle typical problems. This assessment level requires the approach and processes to be well understood and documented. Limited management oversight will be required.

- C. **Likely:** Your approach and processes may mitigate this risk, but workarounds will be required (~50% chance that it **WILL** happen).

A negative outcome is likely, or the current approach and processes are only partially documented. Alternative plans or methods exist to achieve an acceptable outcome even if the risk is realized. Present plans include adequate margins (technical, schedule, or cost) to implement the workarounds or alternatives to overcome typical problems. Significant management oversight will be required.

- D. **Highly Likely:** Your approach and processes cannot mitigate this risk, but a different approach might (>2/3 chance that it **WILL** happen).

A negative outcome is highly likely to occur, or the current approach and processes are not documented. While alternative plans or methods are believed to exist to achieve an acceptable outcome, there are not adequate margins (technical, schedule, or cost) to implement the workarounds without impacting the program management reserves in performance, schedule, or cost. Significant management involvement is required.

- E. **Nearly Certain:** Your approach and processes cannot mitigate this type of risk; no known processes or workarounds are available (>90% chance that it **WILL** happen).

A negative outcome is going to occur with near certainty. No alternative plans or methods have been documented. Alternatively, the risk item has yet to be evaluated adequately to be well understood, so there is a high level of uncertainty about the program success. Urgent management involvement is required.

Figure 4.10-9. Risk Likelihood Definitions

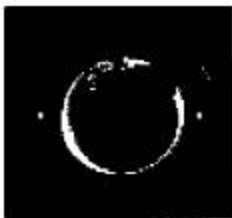


FAA Technical Consequence Definitions

Given the risk becomes real, what would be the magnitude of the impact on system performance?

1. Low: Given that the risk is realized, there would be minimal impact.
A successful outcome is not dependent on this issue; the technical performance goals will be met. There would be no impact on the success of the program.
2. Minor: Given that the risk is realized, there would be a minor performance shortfall but the same approach could be retained.
The resulting technical performance would be below the goal but within acceptable limits. There would be no need to change the basic design, process, or approach. There would be no impact on the success of the program.
3. Moderate: Given that the risk is realized, there would be a moderate performance shortfall but workarounds would be available.
The resulting technical performance would be below the goal. The basic design, process, or approach could be retained with only minor changes, and the overall system performance would still be acceptable as a result of workarounds such as the reallocation of functions or performance goals. There would be only a limited impact on the success of the program.
4. Significant: Given that the risk is realized, the performance would be unacceptable but workarounds would be available.
The resulting technical performance would be unacceptably below the goal. The design, process, or approach would require a significant change to achieve an acceptable performance level. Additional workarounds such as the reallocation of functions or performance goals could also be required. The success of the program could be jeopardized.
5. High: Given that the risk is realized, the performance would be unacceptable with no known workarounds.
The resulting technical performance would be unacceptably below the goal. There are no known alternatives or solutions. The success of the program would be in doubt.

Figure 4.10-10. Technical Consequence Definitions



FAA Schedule Consequence Definitions

Given the risk becomes real, what would be the magnitude of the impact on the schedule?

1. **Low:** Given that the risk is realized, there would be minimal impact.
The program schedule is not dependent on this issue. There would be no impact on the success of the program.
2. **Minor:** Given that the risk is realized, additional activities would be required to meet key dates.
One or more key dates in the program schedule, but not critical path events, would be jeopardized; there are identified schedule workarounds that would be sufficient to mitigate the schedule impact. There would be no impact on the success of the program.
3. **Moderate:** Given that the risk is realized, there would be a minor schedule slip, and one or more need dates would be missed.
One or more key need dates in the program schedule, but not critical path events, would be at least one month late; there are identified schedule workarounds that would be sufficient to keep the program critical path from being affected. There would be only a limited impact on the success of the program.
4. **Significant:** Given that the risk is realized, the program critical path would be affected.
One or more events on the program critical path would be at least one month late. There are identified schedule workarounds that would be sufficient to meet major program milestones. The success of the program could be jeopardized.
5. **High:** Given that the risk is realized, a key program milestone cannot be achieved.
Completion of a key program milestone would be late, and the success of the program would be in doubt. The slip requires a re-baseline of the program.

Figure 4.10-11. Schedule Consequence Definitions



FAA Cost Consequence Definitions

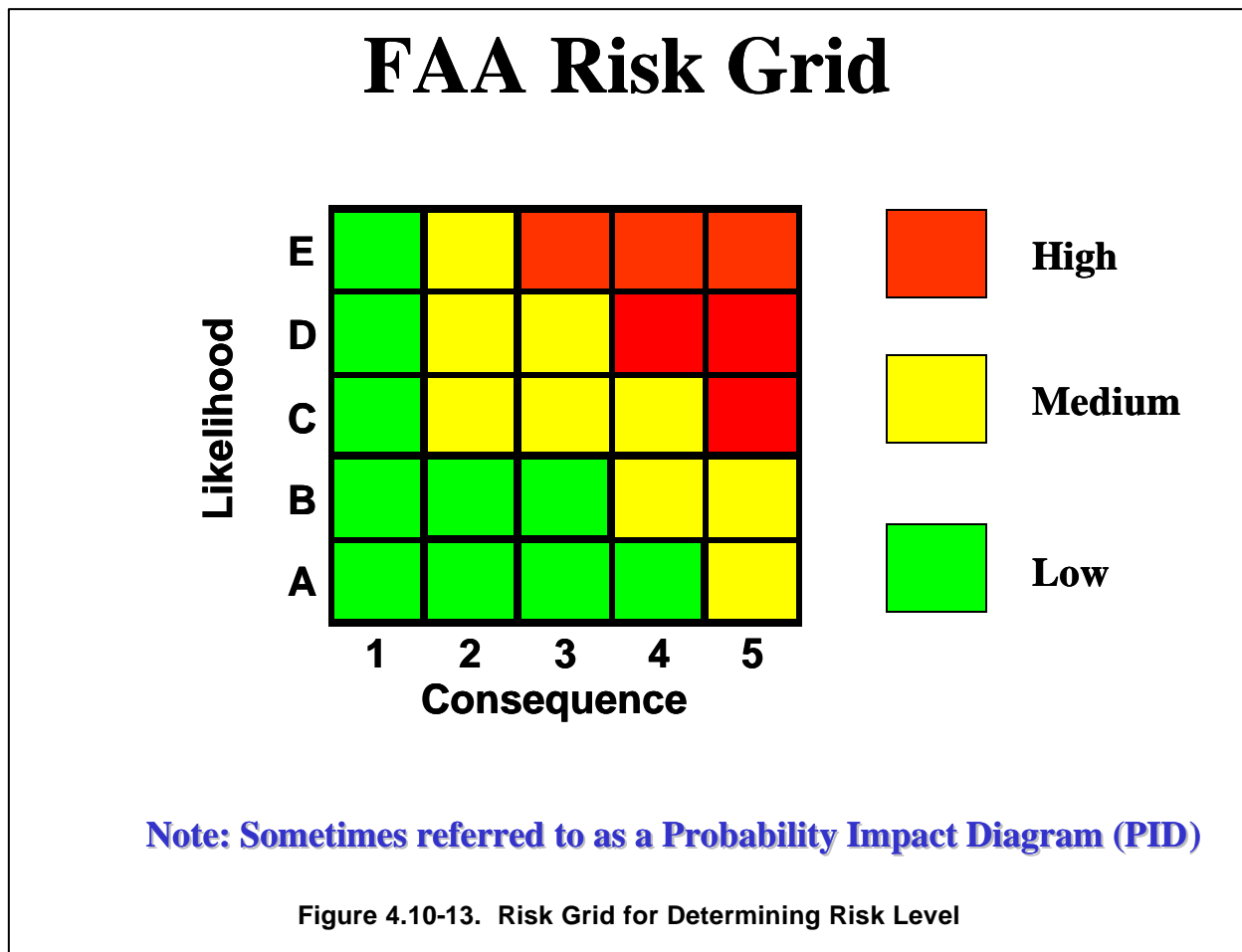
Given the risk becomes real, what would be the magnitude of the impact on cost?

1. Low: Given that the risk is realized, there would be minimal cost impact.
Program cost is not dependent on this issue. There would be no impact on the success of the program.
2. Minor: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by = 1%.
The program costs and/or the production unit cost would increase by = 1%. There would be no impact on the success of the program.
3. Moderate: Given that the risk is realized, there would be a minor increase in financial need. The program costs, operating cost or unit production cost could increase above 1% up to = 5%.
The program costs and/or the production unit cost would increase above 1% to = 5%. There would be only a limited impact on the success of the program.
4. Significant: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by above 5% to = 10%.
The program costs and/or the production unit cost would increase above 5% to = 10%. The success of the program could be jeopardized.
5. High: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by greater than 10%.
The program costs and/or the production unit cost would increase by greater than 10%. The success of the program would be in doubt.

Figure 4.10-12. Cost Consequence Definitions

4.10.3.2.3 Risk Level Determination

The likelihood and consequence are considered to be independent, but are tied to the same event. They are mapped into a risk grid (sometimes referred to as a Probability Impact Diagram (PID)) to determine the individual risk level (e.g., high (red), medium (yellow), or low (green)) as shown in Figure 4.10-13. This mapping facilitates prioritization and trend analyses of risks throughout the life of the program. Use of a color code for each risk level definition supports



effective communication of program health internally and externally, and it is recommended that it be determined early in the life of the program. In some instances, a “risk value” can be computed as the product between the likelihood value and the consequence. This metric is then used to establish a rough priority ranking of the risks.

The construct of a strong risk statement is presented in subsection 4.10.3.1.3 above. As shown in Figure 4.10-13, the “if” portion of the statement maps to the vertical axis of the grid shown, and the “then” portion maps to the horizontal axis. If the risk statement is framed properly, the assessment and subsequent decisions on how to deal with the risk become straightforward.

Risk level definition “**High**” (red) is likely (a high probability) to cause significant disruption of schedule, increase in cost, or degradation of performance. Concerted and continual emphasis and coordination may not be sufficient to overcome major difficulties. “**Medium**” (yellow) may cause some disruption of schedule, increase in cost, or degradation of performance. Special emphasis and close coordination is probably sufficient to overcome difficulties. “**Low**” (green) or

“Basic” (OMB terminology for the same level) has little potential for disruption of schedule, increase in cost, or degradation of performance. Normal emphasis and coordination is probably sufficient to overcome difficulties. The threshold for differentiating between high, medium, and low may change slightly from program to program, but not from risk to risk on the same program or organization.

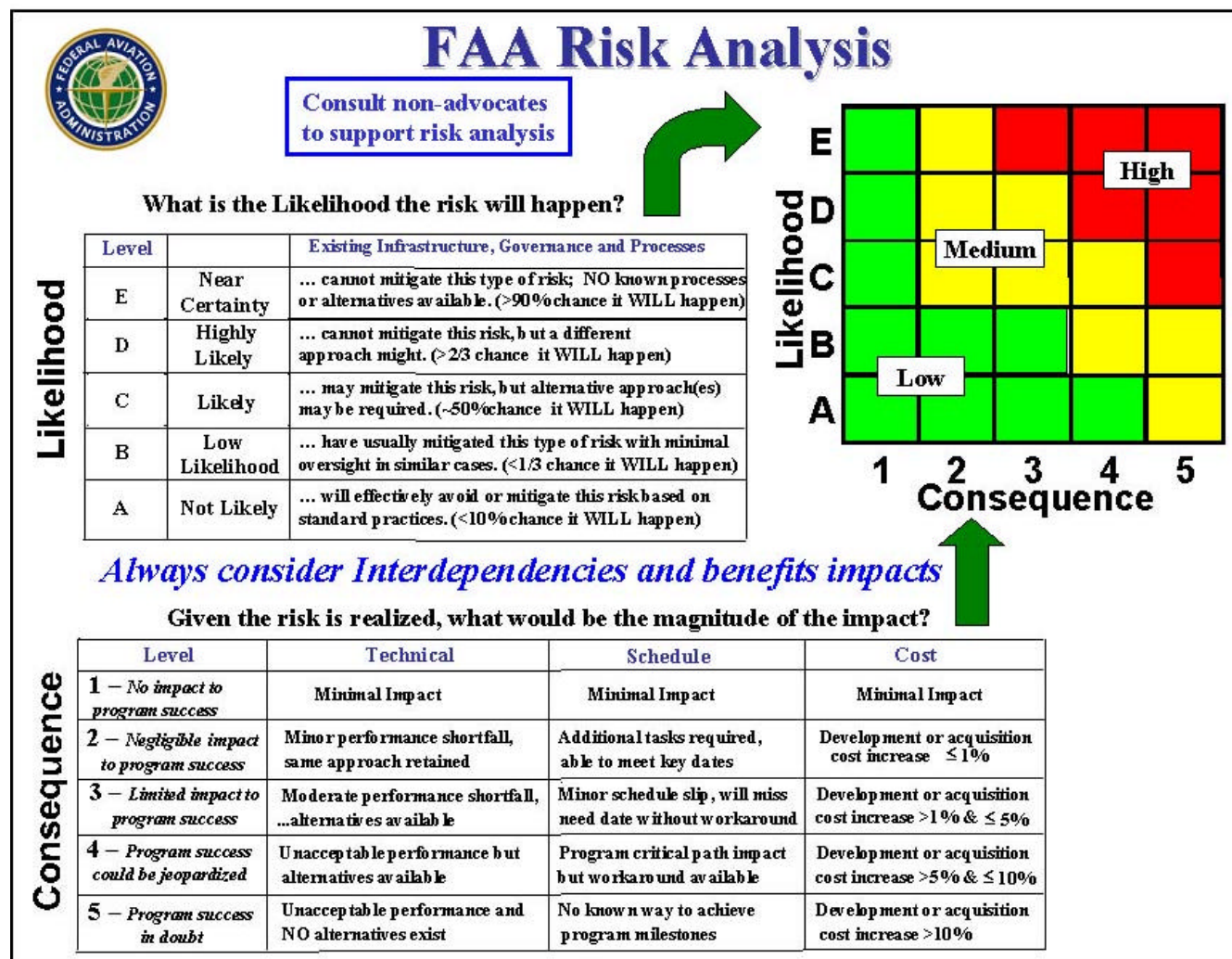


Figure 4.10-14. Risk Analysis



The color coding on this grid is also used to communicate management’s threshold of risk acceptability. For acquisition or development programs, this threshold is usually the line between green and yellow. While development programs are focused on maturing a point solution for a requirements set, research is aimed at determining the feasibility of an approach or technology. For research programs, the level of acceptability is typically defined as the threshold between yellow and red because the success criteria of research do not require the same degree of granularity as development. The degree of risk level acceptance and the actions required to reduce a risk below that level shall be detailed in the Risk Management Plan.

Figure 4.10-14 summarizes how the consequence and likelihood are consolidated to define the risk level.

Various technical communities employ risk analysis techniques or methodologies specific to their domain. They portray their conclusions and recommendations as grids similar to that shown in Figure 4.10-14; but the scales vary from 3 x 3 to 10 x 10 with many variations in between. It is recommended that the representation a given specialty community (such as Safety or Information Security) uses to draw conclusions be suited to its particular situation. However, the criteria used and portrayal of a community's conclusions and/or recommendations shall be consistent with the program or organizational view of risk. Figure 4.10-15 illustrates this correlation for the Information Security Engineering risk elements in Figure 4.8.6-5 (see Section 4.8.6, Information Security) and the basic risk elements discussed in this section. Regardless of the steps/methodologies used by a specialty knowledge domain, all risks need to be portrayed to management on the same basis (see Section 4.10.3.5 below) to allow for effective decisions on the application of risk reduction resources. However, the basic conclusion(s) reached by the specialty community must be preserved in any translation into a common program reporting format.

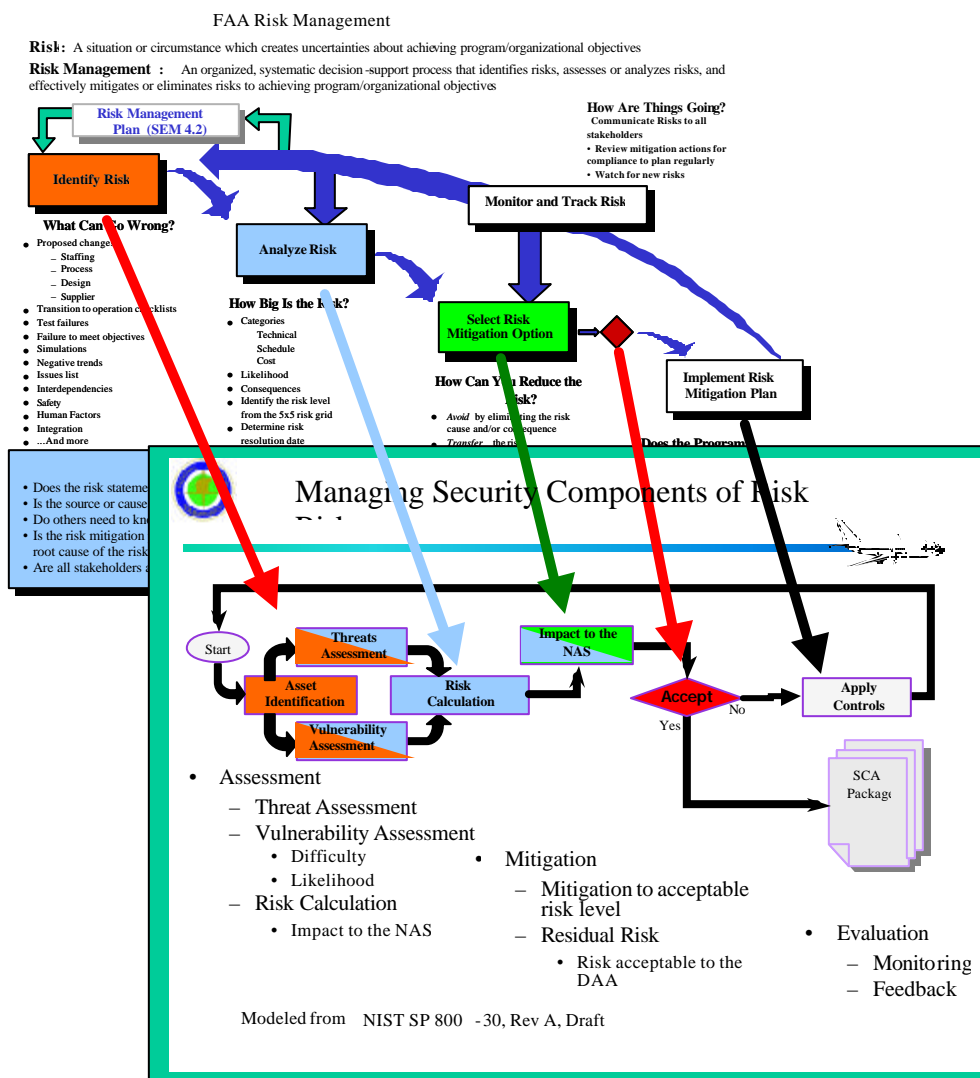
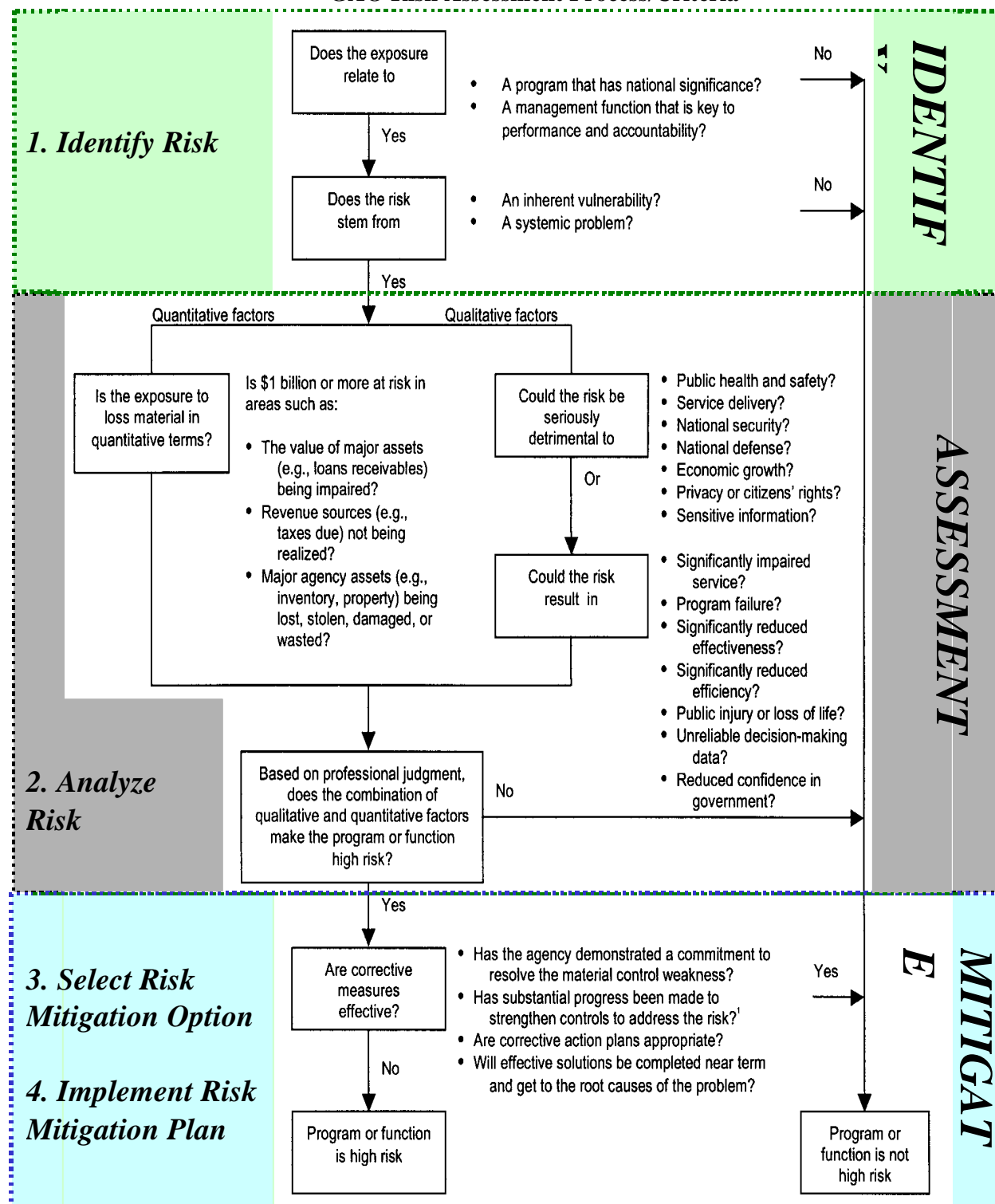


Figure 4.10-15. Correlation of Risk Management With Information Security Methodology

GAO Risk Assessment Process/Criteria



GAO process requires examination of risk and the development of a mitigation effort. Shown is Figure 5 of GAO/OCG-00-12, Page 9. (August/2000).

Figure 4.10-16. Correlation of GAO Recommendations With FAA Risk Management

The Government Accountability Office (GAO) [formerly the General Accounting Office] has also defined a process to handle risk in a report issued in 2000 (see item 16 in References at the end of this section). It contains the same elements in the FAA Risk model except the track and control step. Figure 4.10-16 shows the correlation between the two approaches and demonstrates how the GAO recommendations are satisfied with the process described in the FAA System Engineering Manual (SEM).

4.10.3.3 Task 3: Select Risk Mitigation Option (*Satisfies iCMM BP 13.05 criteria*)

The objective of risk mitigation or risk reduction efforts is to implement appropriate and cost-effective risk mitigation plans to reduce or eliminate the risks. Appropriate risk mitigation techniques are selected and mitigation actions are developed, documented, and implemented. Risk mitigation handling (planning, implementation, and tracking) is the core of risk management. Risk mitigation implementation requires a conscious management decision to approve, fund, schedule, and implement one or more risk mitigation actions. Risk mitigation plans and mitigation actions are reviewed frequently at major reviews, program reviews, acquisition reviews, and milestone reviews.

Risk mitigation actions fall into one, or a combination, of the following strategies:

- Avoidance
- Control
- Assumption
- Transfer (sometimes referred to as “influence”)
- Research and Knowledge

Avoidance is a strategy to avert the potential of occurrence and/or consequence by selecting a different approach or by not participating in the situation that potentially generates the risk. This technique may be pursued when multiple technical or programmatic options are available. It is more likely used as the basis for a go/no-go decision at the start of a program. Some examples are selection of state-of-the-practice rather than state-of-the-art technologies and prequalification of suppliers. The avoidance of risk is from the perspective of the overall program/project, which includes the stakeholders, contractors, and execution groups. Thus, an avoidance strategy is one that involves all of the major parties to the program/project and permits a program/project-wide avoidance of the risk.

Control is a strategy of developing options and alternatives and taking actions that lower or eliminate the risk. This is the most common approach used to handle risks. The objective of this strategy is to take action or make a decision to lessen the probability of occurrence and/or the impact if the risk were to occur. Examples include new concepts, additional technical analysis, redundant systems and/or components, and alternate sources of production.



Refer to Table 4.10-6 for more information on choosing control as the risk handling approach.

Table 4.10-6. Sample Risk Handling Strategies

Typical Risk Control/Mitigation Approaches
<ul style="list-style-type: none"> • Multiple development efforts • Extensive alternative design studies • Trade studies — technological development verses operational impact • Early prototyping • Incremental/Evolutionary/Spiral development • Technology maturation efforts • Robust design • Reviews, walkthroughs and inspections • Open Architecture and Systems • Use of standard items (COTS)/software reuse • Use of engineering mockups • Modeling and simulation • Key parameter control boards • Manufacturing screening (Environmental Stress Screening)

Assumption is simply accepting the likelihood/probability and the consequences/impacts associated with a risk's occurrence without engaging in any special efforts to control it. Assumption is usually limited to low risks. This is a program/senior management option, not a practitioner option. FAA practice for investment programs is to develop mitigation plans for all medium and high risks. However, the actions required to address individual risks shall be contained in the governing RMP.

Transfer is a strategy to shift the risk to another area, such as another requirement, an organization, a supplier, or a stakeholder. Examples include reallocating requirements, securing supplier product warranties, and negotiating fixed-price contracts with suppliers. Note that at the program or higher organizational level, the risk remains; the transfer of the risk is accomplished primarily to optimize the overall program risk and to assign ownership to the party most capable of reducing the risk. Risk cannot be transferred unless the recipient agrees to accept the risk. It is possible that the risk level may change as a result of the risk transfer.

Research and Knowledge may mitigate risk through expanding research and experience. Since risk arises from uncertainty and inexperience, it may be possible to effectively mitigate risk simply by enlarging the knowledge pool, leading to reassessment that reduces the likelihood of failure or provides insight into how to lessen the consequences.

At this point, several alternatives for mitigating the risk have been identified and analyzed for selection of the preferred approach. Alternatives include detailed plans for mitigating the risk in several small, sequential steps; alternative steps; or entirely new (non-baselined) approaches to accomplishing the program. Further, contingency plans are identifiable alternatives, which may be implemented if a mitigation plan fails, and the risky event or conditions occur with more

serious consequences than anticipated. The mitigation steps are the major milestones of the mitigation plan. Contingency plans need not be detailed until they become the primary approach to reducing the risk.

For instance, the risks associated with selecting a COTS-based acquisition approach (see Figure 4.10-6) have known risk mitigation strategies. These strategies need to be included in the trade studies when comparing investment or acquisition approaches. Because COTS has an inherent set of risks that are market driven, most of the risk mitigation strategies fall into the “Control” category in order to anticipate and reduce the risks to acceptable levels. More information on COTS risks and mitigation strategies may be found in the FAA COTS Risk Mitigation Guide, which is available at <http://www.faa.gov/aua/resources/COTS>.



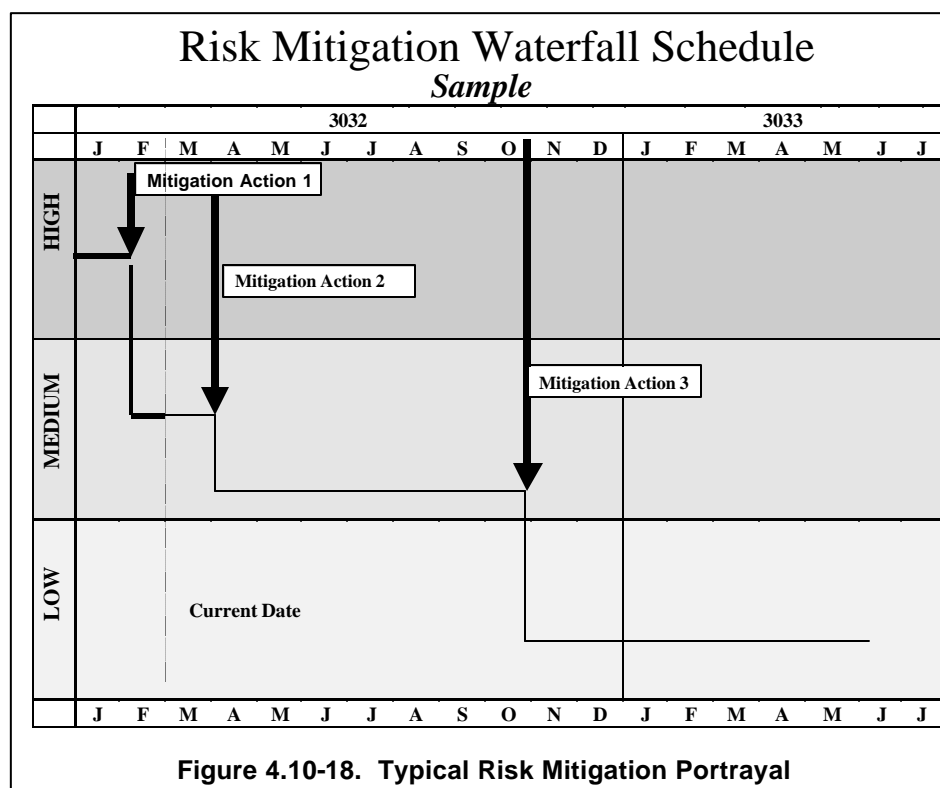
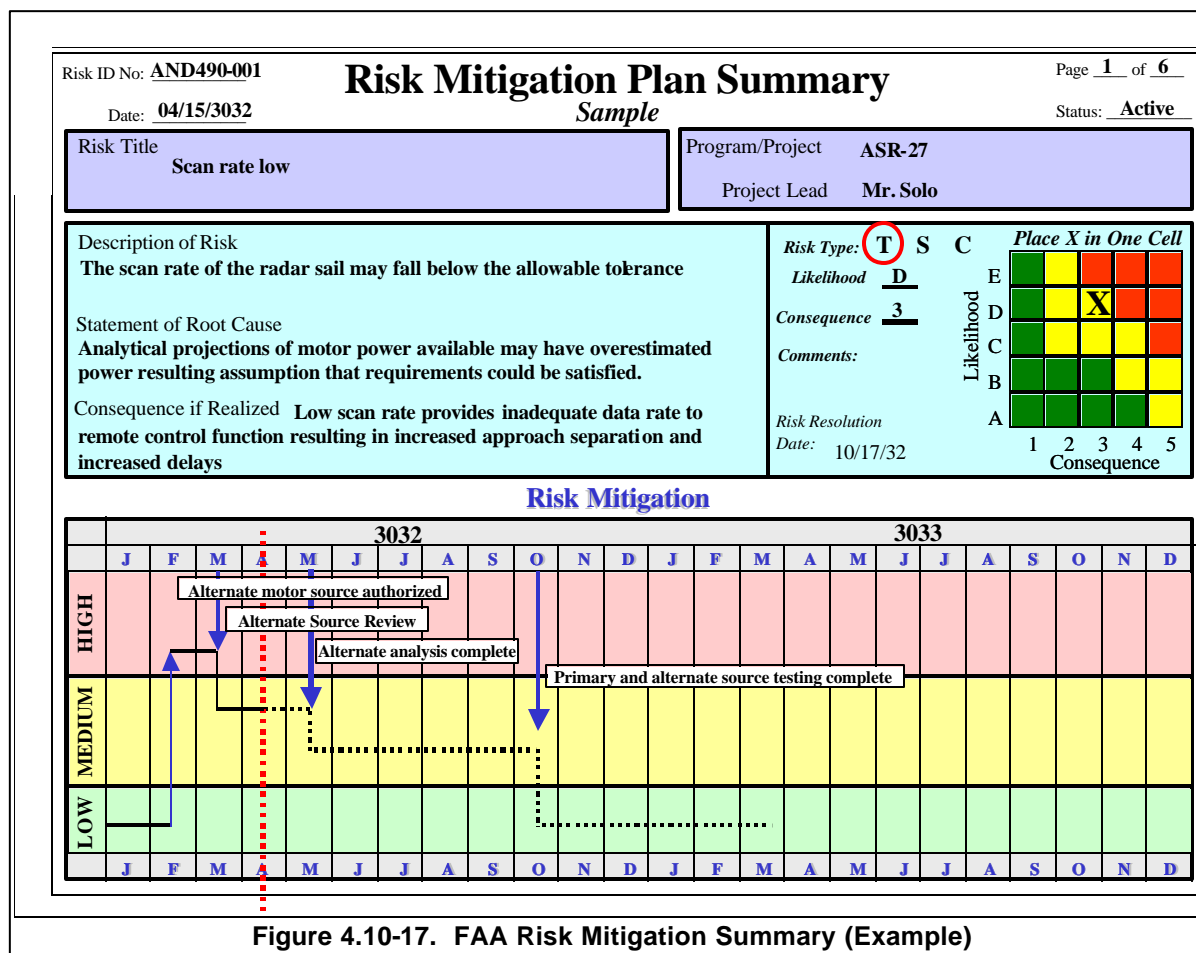
Trade study techniques may be performed to help select the preferred risk mitigation plan. While the proper criteria and their weights for each analysis are dependent on the risks to be mitigated, it is recommended that the following considerations be included:

- Does the option mitigate the likelihood or consequence of the risk?
 - Does the option fit within program/organization's scope?
 - Is the option easy to implement?
 - Are new risks avoided or introduced as a result of the mitigation?
 - What is the cost of mitigation?
 - What is the schedule for mitigation?
 - Is the recommended course of action an acceptable approach to management?
- While this implies some limitations on the choices considered, it should **NOT** preclude an approach not used before **IF** solid rationale can be offered to support it.

The risk level is the first criterion used to determine the need for a risk mitigation plan. As specified in the RMP, risks that typically fall into the medium or high categories require risk mitigation plans. Risks that are assessed as low typically do not require mitigation plans but may have certain aspects that would be prudent to monitor. If this is the case, risk mitigation plans may be formally or informally implemented for these low risks based on the specific governing RMP.

It is essential that those responsible for plan implementation have a thorough understanding of the root cause of the risk to be mitigated. This may be accomplished with a good summary statement of the risk (see subsection 4.10.3.1.3). Do not state the risk in terms of its mitigation plan. It is recommended that the status also include a summary of risk mitigation efforts that references more detailed documentation. A Risk Mitigation Plan Summary (Figure 4.10-17) is used to report the analysis and actions on an individual risk.

The risk mitigation plan documents the specific steps to be implemented, the sequence in which they are to be implemented, and the points in time at which they are to be implemented. Developing a risk mitigation plan includes assessing the expected outcome following implementation. It is recommended that the same method initially used to assess the risk, such as risk templates, be used to provide a forecast of the risk level after completion of each action of the risk mitigation plan. The expected impact of each mitigation event on risk level may be projected using a format similar to that of Figure 4.10-18 (a waterfall, or “burn down,” chart).



The risk mitigation plan becomes the basis for monitoring success in reducing each risk to an acceptable level. The plan includes, but is not limited to, the following:

- A description of the risk for which the plan applies
- Mitigation approaches which detail the specific actions that are planned to reduce the risk or eliminate it. It is recommended that these actions be event based, integrated into a schedule, and have associated with each of them:
 - The decision point or trigger, past or future, that initiates the action or group of actions
 - Resources required to execute the actions (including personnel, capital equipment, facilities, procured equipment)
 - Measures of success to be used for the planned actions or group of actions
 - Fallback options or contingency plans (if any)
 - Planned completion dates of the actions
- Risk mitigation metrics
- The Risk Worksheet (Figure 4.10-7)
- The initial Risk Mitigation Plan Summary (Figure 4.10-17)
- The Risk Mitigation Waterfall Schedule (Figure 4.10-18)

A risk mitigation plan must be periodically evaluated to determine its effectiveness. This analysis is performed in the same manner as initial analysis for the risk. The set of templates used for analysis of the risk may also be used to determine the mitigation in the risk level following completion of each major action or group of actions. The regular reassessment of the risk and performance-to-plan using a fixed set of criteria provides a consistent analysis of the impact to the program.

An effective technique is to indicate in advance how successful completion of the actions outlined in the Risk Mitigation Plan affects the risk. Not all actions have a comparable impact. Some actions or decisions provide the basis for others to be effective. In contrast, certain events, actions, or decisions have a fundamental impact on the level of risk remaining, both from a positive and negative perspective. A “best practice” can be illustrated when the mitigation plans for several of the examples of strong risk statements discussed in subsection 4.10.3.1 are reviewed (details have been changed for illustrative purposes):

Our first example of a strong risk statement (Risk #216) stated: “If either the multiple SMR SAT completion or the start of the ASDE-X Safety Logic Optimization by July 15, 2006, is delayed in any way, then the commissioning of the new Atlanta ATCT and the IOC date of May 1, 2007, will be delayed, which will not meet the terms of the AT/NATCA MOU.”

This was initially assessed as a high (red) risk, which means that effective action needed to take place to reduce it. The mitigation strategy recommended and accepted was threefold: (1) to monitor the sensor and safety logic development progress with each system enhancement, (2) manage the results to realistic expectations, and (3) pursue a single sensor configuration in lieu of multiple sensors to reduce complexity and associated cost/schedule. To implement this strategy, the program put the following actions and schedule in place:

- 12/01/05: Monitor Safety Logic Test and Development activities in MCO. Note: Unsuccessful IOT&E at MCO could impact Atlanta Safety Logic testing start.
 - 02/26/06: Track schedule of Single SMR Optimization to ensure that it is on schedule. Measure remaining schedule to see if allotted time available is sufficient to complete Multiple SMR optimization. If not, by 5/13/06, accelerate optimization efforts of FAA field personnel and vendor.
 - 05/13/2006: Multiple SMR optimization start — poor performance will trigger single SMR contingency.
 - 07/2006: Safety Logic optimization start *(trigger to reassess risk)*.
 - 10/2006: Formal SAT start *(trigger to reassess risk)*.
 - 02/2007: Safety Logic optimization and test *(trigger to retire risk)*.
- (Risk last reviewed 11/2005)

In our second example (Risk # 305), the risk statement read: “If the Safety logic design and associated performance does not meet the operational expectations at Orlando International (MCO), then the ability to achieve ISD and deploy at other sites per the deployment schedule will be at risk with continued potential of accidents caused by runway incursion incidents at those locations.”

This was assessed as a high (red) risk. A mitigation strategy to define requirements for operational expectations and conduct software code reviews, data analyses, and Operational Tests (OT) to assess system performance was developed, and the following detailed actions were put in place:

- 03/23/2006: Define operational expectations.
- 07/27/2006: Collect operational data for future data analysis.
- 10/29/2006: Conduct shadow operations with users to identify areas of concern.
- 02/14/2007: Identify design and adaptation changes to improve system performance *(trigger to reassess risk)*.
- 03/2007: Conduct additional shadow operations testing to identify needed improvements.
- 05/06/2007: Conduct operational test to assess performance and identify potential system changes *(trigger to reassess risk)*.
- 07/8/2007: Use Tech Center lab to analyze results from shadow operations and OT.
- 07/2007: Conduct software code reviews to verify functionality.
- 09/2007: Conduct full IOT&E at MCO *(trigger to retire risk)*.

(Risk last reviewed 11/2005)

In our final example, (Risk # 389), a medium (yellow) risk level was assigned to the risk statement: “If adjustments are not made to the installation schedule to accommodate aggressive intervals for key activities, the ASDE-X system may be in jeopardy to meet the

Operational Required Date at Seattle International in time to support the decommissioning of ASDE-3 in August 2007, as required in the MOU with the Port of Seattle.”

The plan adopted involved compressing the remaining available schedule by adding resources. The details of this plan involved the following actions:

- 10/2005: The resources assigned to site preparation have been increased. A 3-person team was instituted for the months of April through October 2005, which helped to absorb loss of time for site preparation activities (i.e., added resources to the project instead of extending schedule) **(complete)**.
- 10/22/2005: Site prep **(complete)**.
- 04/2006: Optimization of Remote Units and SMR planned complete **(trigger to reduce risk rating)**.
- 10/2006: IOT&E.
- 01/2007: Field performance evaluation complete.
- 06/2007: Achieve IOC **(trigger to retire risk)**.

(Risk last reviewed 11/2005)



In addition to the attributes of a strong risk statement described in subsection 4.10.3.1.3, the characteristics of an effective mitigation plan illustrated in each of these examples include:

- A strategy or approach that traces directly to the problem statement, and, therefore, addresses the root cause of the risk rather than symptoms
- Defined and measurable actions that are integrated into the Integrated Master Schedule (IMS)
- Triggers to reassess risk level and progress to plan
- Currency of risk information (both status and date last reviewed)
- Interdependencies that impact the effectiveness of individual mitigations

The Risk Worksheet (Figure 4.10-7) guides the practitioner through the first three tasks in the Risk Management process: Identify, Analyze, and Develop mitigation planning to obtain a risk reduction decision. When a risk mitigation plan has been prepared, management reviews and approves it based on criteria defined in the RMP. The decision is reflected in the disposition blocks at the bottom of the Risk Worksheet.

4.10.3.4 Task 4: Implement Risk Mitigation Plan (*Satisfies iCMM BP 13.05 criteria*)

Once the organization decides on a risk mitigation approach and supporting actions, the decision shall be implemented and carried out effectively so that either risk likelihood or consequence, or both, are reduced to an acceptable level. Risk reduction implementation requires that the associated specific tasks be incorporated into the planning, scheduling, budgeting, and cost-accounting systems used by the program or in the implementing organization. Incorporating risk mitigation actions directly into the overall program schedule at a point where risk likelihood or consequence may be affected before a risk occurs keeps management and the program team/organization aware of the need to allocate resources (labor, materials, and possibly other resources) to accomplish the authorized risk reduction. The Risk Mitigation Plan Summary chart (Figure 4.10-17) is used as a means of reporting

progress in reducing risks. Each major event in the mitigation plan is identified along with how that event reduces the risk and to what extent.

Incorporating the risk mitigation plans and milestones into program and organizational processes and systems ensures that the risk and its mitigation plans may be monitored and tracked until the risk is eliminated, or the risk requires program modification. Risk mitigation plans may be documented starting with the Risk Worksheet (Figure 4.10-7) and a Risk Mitigation Waterfall Schedule (Figure 4.10-18). Mitigation activities are shared with and communicated to all stakeholders.

4.10.3.5 Task 5: Monitor and Track Risks (*Satisfies iCMM PA 14 criteria*)

Because risk is dynamic, continual attention of all involved is necessary regarding how the risk profile is changing based on events, decisions, and actions on the project. Reassessing currently managed risks is done on both a periodic and event basis to reflect current status of the risks as well as to identify and quantify new and emerging risks. The SE milestones and quality gates discussed in Integrated Technical Planning (Section 4.2) provide formal checkpoints for management insight into the risks as well as achievements to date. There will be additional opportunities for project personnel to periodically status risk as outlined in the RMP. New potential risks to the program may be identified at any time. Newly identified risks are analyzed using the same steps described in subsection 4.10.3.2.

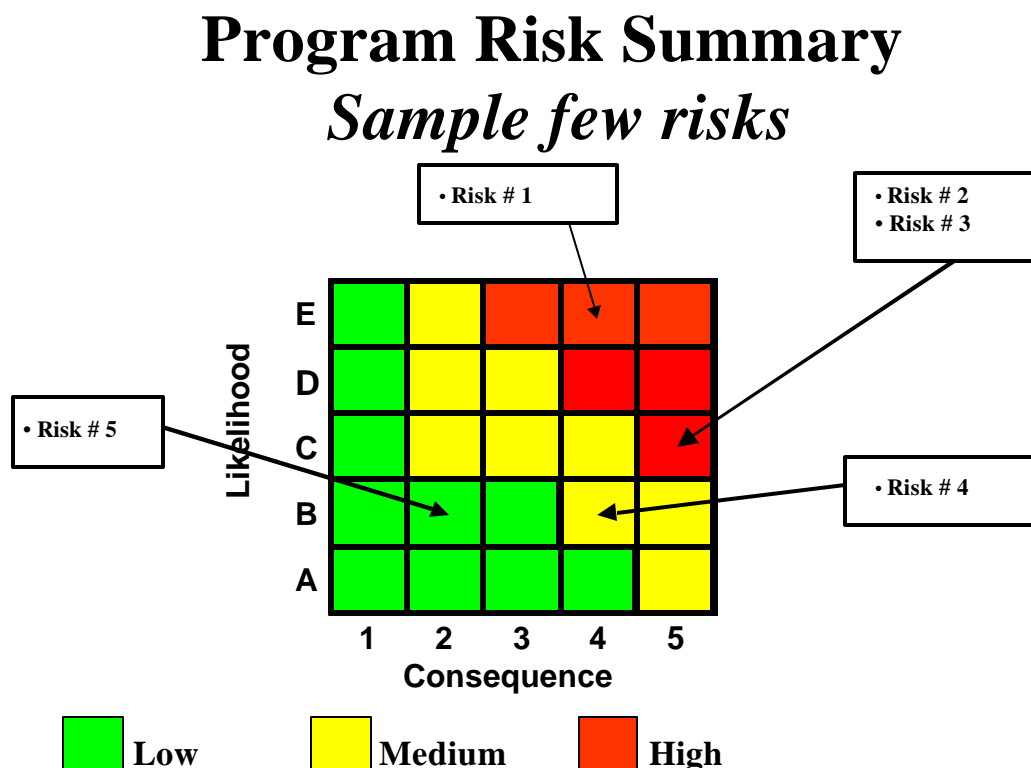


Figure 4.10-19. Aggregate Risk Grid

Steps in the risk-tracking process focus on providing program risk trends and status to the execution teams, interdependent activities, and program management. Actual performance of the planned mitigation actions is compared to the expected performance. The bold line on the Risk Mitigation Plan Summary “waterfall area” (see Figure 4.10-18) indicates progress made to date on the mitigation plan. Detailed cost and schedule tracking is done as part of the program

schedule and cost-tracking system. To ensure consistency across the program/organization, the governing RMP shall contain the management visibility requirements for the program. These requirements include reporting frequency and content.

A sample of a brief summary of all risks for a particular program (or team) with relatively few risks is displayed on an aggregate risk grid (or Probability Impact Diagram) shown in Figure 4.10-19. A standard reporting format shall be used (see Figure 4.10-20) to facilitate integration of risk information across projects and programs. It is recommended that the risk management plan also indicate the extent of required supporting detail, usually in the format of templates (see Figure 4.10-21). It is recommended that the management visibility effort be focused on monitoring and tracking the effectiveness of the risk reduction decision. The impact of the risk on the program and the relevant **decision** are incorporated into the project schedule as risk mitigation actions. They are inserted into the program's Integrated Master Schedule (Figure 4.10-22). The lowest level tasks involved are flagged with the assessed risk level; higher-level Work Breakdown Structure (WBS) tasks inherit the maximum risk level present in any subordinate task. Hence, review of the schedule at any level from summary tasks (Figure 4.10-22, top) to lowest level tasks (Figure 4.10-22, bottom) allows program management to maintain appropriate risk visibility and also allows "drill down" to increasing levels of detail as the schedule view is expanded.

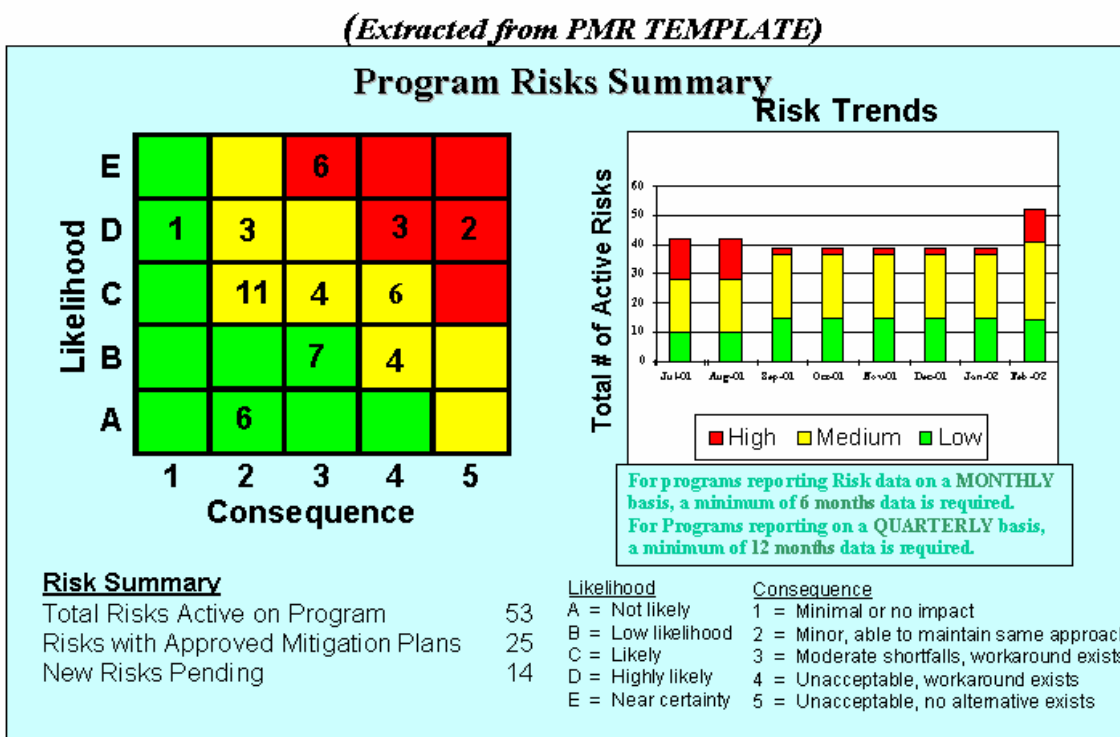


Figure 4.10-20. Standard Risk Reporting Format

(Extracted from PMR TEMPLATES) Program Risks

Risk Level	Risk #	Likelihood	Impact	Risk Item	Mitigation Strategy	Risk Mitigation Decision Date
H	46	E	4	TS IF TSOs and ACs are delayed, THEN the standards will not support mandated deployment dates.	PT will work with industry to secure support	Jan-01
H ▶	14	D	5	C Aerospace User Coordination – IF GA Aircraft users do not accept NEXCOM plan - Benefits for GA not sufficient to engender support - Low end GA Avionics costs too expensive	PT reps will meet with reps of the GA community to determine concerns and strategies for resolution of concerns.	Jun-02
H ▲	30	D	5	C IF Business case does not demonstrate ROI, THEN airlines won't equip.	PT will establish joint working group with industry to develop business case that industry can support.	Jul-02

List risk updates IN PROGRAM PRIORITY ORDER for each New, High Risk item (Red), and Significant Level Changes (High to Low &/or Low to High).

Likelihood

E = Near certainty
D = Highly likely
C = Likely
B = Low likelihood
A = Not likely

Consequence

1 = Minimal or no impact
2 = Minor, able to maintain same approach
3 = Moderate shortfalls, workaround exists
4 = Unacceptable, workaround exists
5 = Unacceptable, no alternative exists

Risk Level:

H - High M - Medium L - Low
 ▶ = same as last report
 ↓ = down from last report ▲ = up from last report

Risk Type

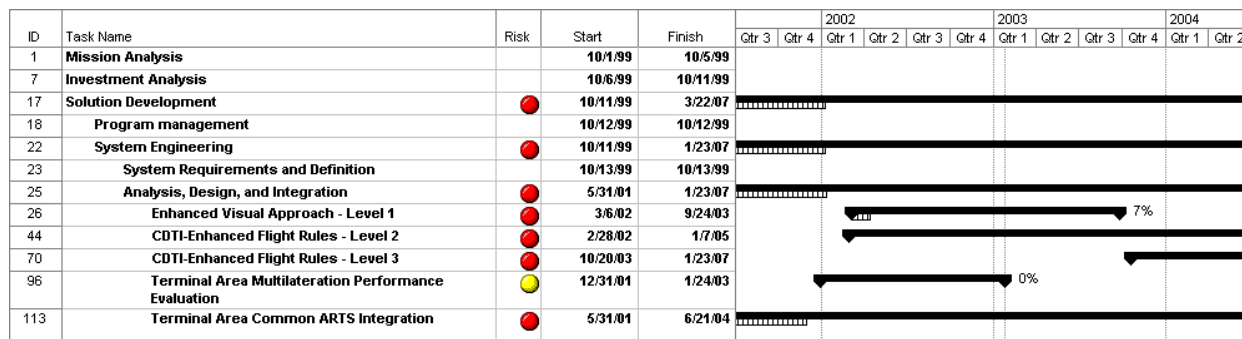
T = Technical
S = Schedule
C = Cost

Note: There is a difference between a risk and an issue. If something is a certainty, it is no longer a risk and should be described as an issue and reported on the issues/concerns slide

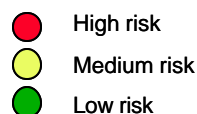
Initially each High risk should be briefed. Subsequently, any new or major change to a risk item should be captured on this slide. See attached proposed "Risk Management" (Attachment #1) for guidance on how to assess and report program risks.

Figure 4.10-21. Template Formats

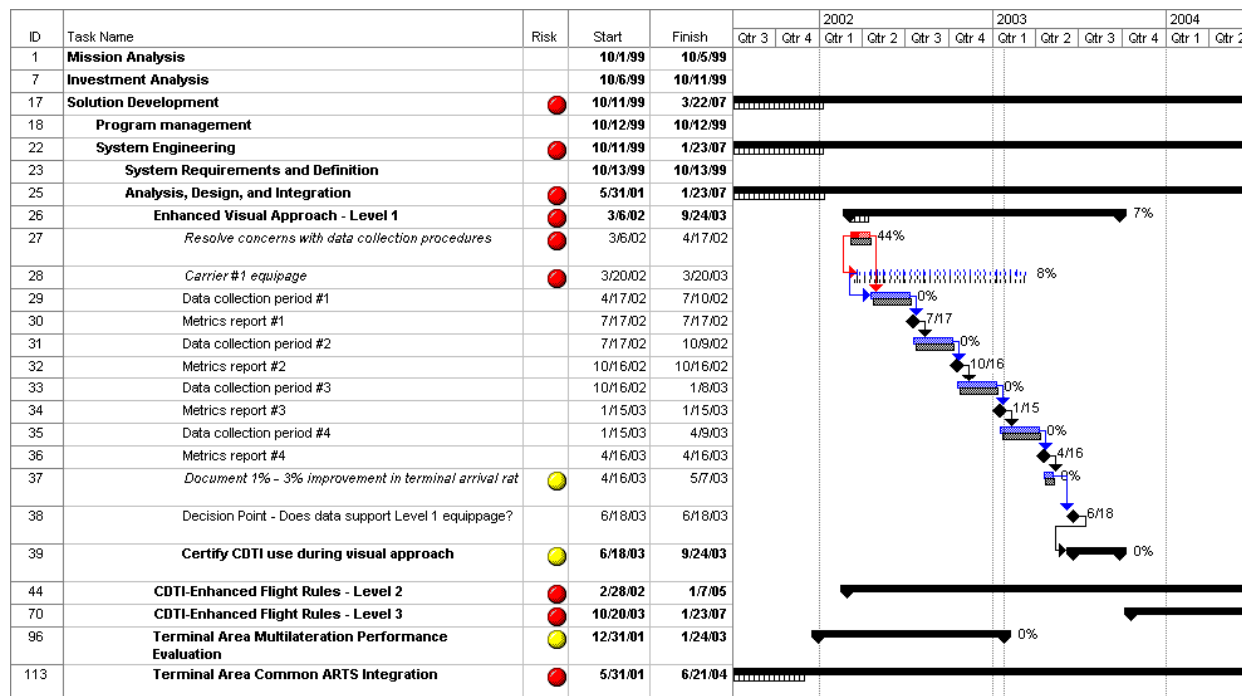
Integrated Program Schedule: summary level (top) and “drill down” to lowest level tasks



Risk information displayed at summary task level in the program Integrated Master Schedule (IMS)



(bottom).



Drill down capability – Risk information displayed for lowest level tasks;
summary tasks show highest level of risk for any subordinate task

Figure 4.10-22. Risk Information Incorporated Into Program



Effective program management always involves examining cost and schedule during review of the progress of the program. Making risk information visible as part of the IMS through linkage with each WBS element affected ensures that risk information receives ongoing management attention. Integrating program risk data into the integrated master schedule fosters better, risk-based decision making in at least five ways:

- The need for separate risk reviews competing for the program manager's time and energy is eliminated.
- Integrating the risk information into the IMS effectively prevents isolation of the risk efforts from the mainstream tasks and program milestones. The risk profile of the program is presented as part of the overall management view of the program. As each decision point is reached, the risk information associated with that event or WBS element is portrayed, and hence shall be considered.
- The portrayal of program progress illustrated in Figure 4.10-22 alerts management to when a decision needs to be made and what that decision is. This provides visibility across the entire program *in advance* of impending decision points so that the necessary relevant information is provided in a timely manner to support an informed decision.
- OMB requires FAA investments to manage costs and schedules on a “risk-adjusted” basis. Integration of risk information provides objective evidence that schedules and costs accommodate the risks involved.
- Examination of the risks provides insight into mitigations that lead to pursuing potential opportunities.

Major FAA programs must submit yearly budget estimates with supporting justification for the investment in accordance with OMB Circular A-11 (Reference 22). These submissions are provided as an “Exhibit 300” in a format prescribed by OMB. OMB uses risk as a factor to measure the health of investment programs based on the Exhibit 300 data. OMB requires that the risk-related data be presented in various sections of the Exhibit 300 as defined in Circular A-11. Examples where risk should be reflected should be found in the sections discussing life cycle cost estimates, program schedules, privacy, security, and the structuring of major acquisitions. In particular, the cost estimates and schedules for the investment should show how they have been adjusted for the risks associated with the investment. The OMB requirement is to provide objective evidence that all aspects of risk have been considered in managing FAA investments. OMB is looking for “an integrated process within an agency for planning, budgeting, procurement and management of the agency’s portfolio of capital assets to achieve agency strategic goals and objectives with the lowest life-cycle cost **and least risk.**” (Circular A-11 (2006) section 300.3).

Please note that the OMB terminology discussion of “risk contained in risk management plans” (A-11 (2006) section 300.4) refers to risk mitigation plans as discussed in this section of the FAA SEM.

4.10.4 Outputs (*Satisfies iCMM Artifacts criteria*)

Five major outputs of this process that directly influence the program and/or an organization’s decisions are:

- Program Risk Summary (Figures 4.10-20 and 4.10-21)

- Risk Mitigation Plan Summary (Figure 4.10-17)
- Risk Mitigation Plans (see subsection 4.10.3.3)
- Aggregate Risk Grid (Figure 4.10-19)
- Risk Status

It is recommended that the Program Risk Summary, the Risk Mitigation Plan Summary, and the Program Risk Mitigation Progress charts be briefed at all regular program reviews. Management decisions are based on the above information. It is recommended that a complete status of a given risk be briefed when the risk is identified and immediately following the risk realization date. It is recommended that the Risk Mitigation Plans be handled as an integral part of program effort.

4.10.5 Risk Management Tools

The tools needed to implement this process include:

- Approved Risk Management Plan
- FAA Risk Worksheet
- Likelihood and consequence templates for a 5 x 5 PID tailored for the program
- Risk Mitigation Plan Summary
- A means to communicate results across a program (electronic mail, servers, etc.)
- A means to document the results of the process and manage the outputs (databases, spreadsheets, word processors, etc.)
- Analytical tool(s) to support risk analysis and tracking

4.10.5.1 Analytical tools

Analytic tools assist in the assessment and management of risk information. Tool capabilities can range from the simplistic to very complex. Use of a given tool is driven by the needs of the organization's risk management efforts.

If risk can be managed or tracked on an individual basis without a need for integration with other risk efforts, a number of choices are available within the organization's current desktop environment using either word processing or spreadsheet applications. Another choice is a database application, which provides additional features. An example of a standalone or individual user database tool is "Risk Radar" (a tool free to the government that may be used to generate many of the risk work products (see subsection 4.10-4)). A version of Risk Radar that incorporates the FAA templates and forms is available through the System Engineering Council (SEC) sponsored Introduction to FAA Risk Management course (SEC 410). This software is available free to all FAA programs (including contractors for use in supporting FAA programs). It requires MS Access 2000 and interfaces with MS Project 2000 for schedule linkage to the overall program IMS.

If the requirements in the RMP for capabilities that go beyond those described above (such as risk rollup to different organizational levels), then a risk tool suite with network and/or Web capability may be required. There are a number of commercially available tools available that provide an array of capabilities ranging from Web-based entry through organization-wide risk, analytical capabilities, and even opportunity management.

Analytic tools may be used for probabilistic analysis of schedule uncertainty or technical uncertainty. Critical Path Analysis tools may be used with the Integrated Program Schedule to regularly evaluate schedule risk. In a similar fashion, commercial applications (e.g., @RISK) may be applied to technical parameters (such as weight, latency, power, computer throughput) to establish confidence ranges. Results from these probabilistic analyses may support the overall risk analysis task of establishing a likelihood of occurrence. Details on use of probabilistic analysis are not covered here, but may be found in textbooks and technical papers that cover statistical analysis for risk management. For those investments that require an Exhibit 300 to be submitted to OMB, a comprehensive tool suite is under consideration at the time of publication of this update for FAA-wide application. A Risk Management capability is planned to be part of that standard tool suite, especially since schedules and budgets need to be “risk adjusted”.

4.10.5.2 Risk Register

The risk register (see example in Figure 4.10-23) is a listing of risk information associated with achieving program objectives. If risk registers are created and maintained by each project, a single composite register of all interdependency risk items shall be developed for the program. These registers are to be consistently used to monitor and track overall risk status within team meetings, program management reviews, and major program reviews. Immediately following identification and analysis of a new medium or high risk, or when a significant change occurs in a previously identified risk, changes shall be incorporated in the register and other documents and the new risk identified to stakeholders. The distribution list is to be established and documented in the RMP. Computer database systems may be needed to manage these outputs for large programs. Smaller programs may often be able to use desktop computer techniques. At a minimum, the following information shall be included in the risk register:

4.10.5.2.1 Risk Register Identification and Creation/Update Date

This is the name of the program risk item. Indicate the root cause of the risk in this section.

4.10.5.2.2 Risk Identification Number

This number is a code that identifies a unique sequence.

4.10.5.2.3 Likelihood

This is a figure of merit indicating the relative likelihood/probability that the identified risk will actually occur (Likelihood Template, Figure 4.10-9).

4.10.5.2.4 Impact (Consequence)


This is a figure of merit indicating the relative severity of consequences/impacts that could result if the identified risk did occur (Consequences Templates, Figures 4.10-10, 4.10-11, and 4.10-12, for examples).

4.10.5.2.5 Risk Level/Change

This is a single letter indicating the assessed risk an item as high, medium, or low (H, M, L) or, red, yellow, or green (R, Y, G) respectively. An arrow that indicates the direction that the risk has moved since the last revision to the risk register demonstrates the risk change.

4.10.5.2.6 Risk Consequence Description

This is a brief, well-stated description of the risk’s negative consequences.



FAA Program Risk Register

(Example)

DATE 04/15/3032
Page 1 of 1
Revision

Risk	Line	Consequence	Risk Level / Change	Risk Description	Next Milestone Date	Risk Resolution Date	Mitigation	Risk Type
1	4	3	M ↓	Sweep rate low/delays-benefits loss	30320515	30321017	On Track	T
2								
3								

Consequence Key :

1= Minimal impact

2= Minor, able to maintain same approach

3= Moderate shortfalls, workaround exists

4= Unacceptable, workaround exists

5= Unacceptable, no alternative exists

Risk Level:

H - High M - Medium L - Low

→ = same as last report ↑ = up from last report

↓ = down from last report

Risk Type:

Ⓘ - Technical

Ⓒ - Schedule

Ⓓ - Cost

Figure 4.10-23. Risk Register

4.10.5.2.7 Next Milestone Date

This is the projected date at which the risk level converts to lower risk. This is traceable to the Risk Mitigation Plan Summary (Figure 4.10-17).

4.10.5.2.8 Risk Realization Date

This is **the date (or point in time) of the event that either makes the risk a real part of the program or eliminates the need to track the risk.** Early in the program, it may be difficult to predict an exact date, but a general timeframe needs to be developed. As the program matures, date realization occurs. It is recommended that these dates be reviewed regularly and be on the program master schedule.

4.10.5.2.9 Mitigation Status

The currently planned mitigation actions are defined, either explicitly or by reference.

4.10.5.2.10 Risk Type

The risk type designates if the risk is a cost risk, a schedule risk, or a technical risk (see subsection 4.10.3.1.1).

4.10.5.2.11 Risk Mitigation Plan Status

The teams regularly update and report the status of the risk mitigation plan for each risk being tracked that requires risk handling. Actions are initiated as required for mitigation plan activities that are not being accomplished. The risk status is also reviewed with program management on

a regular basis. A sample of a brief summary of all risks for a particular program (or team) is shown in a Program Risk Summary (Figures 4.10-19 and 4.10-20) for use depending on program size.

4.10.6 Risk Management Process Metrics (*Satisfies iCMM PA 18 criteria*)

To be useful, Risk Management-related metrics must be focused on organization and/or project goals and success criteria. The metrics for risk management vary by organization and sometimes by project. Whatever measurements or statistics are used to help manage the project are the best metrics for that project. At the program level, these metrics measure program progress to plan. Earned Value Management (EVM) is an excellent set of measures to portray the extent of schedule and cost risk in a program. The variance to plan for either the Schedule Performance Index or Cost Performance Index may be used as a measure of risk on the program. The EVM reporting requirements in the OMB Exhibit 300 provide a ready means to capture risks of this nature. Technical or performance risk may be measured by using Technical Performance Measures. The projected and/or actual variance to performance requirements is a measure of technical risk. At a lower level, metrics for the Risk Management process itself may include:

- **Total active high risks, total active medium risks over time.** The objective is to provide visibility into risk trends over time.
- **Percent of risks (medium and high) with approved mitigation plans.** The objective is to measure the effectiveness of handling the risks requiring action.
- **Average time span of overdue mitigation activities.** The objective is to measure the effectiveness of meeting mitigation plan schedules.
- **Aging of active risk records.** The objective is to gain insight into the currency of the risk database.
- **Number of risks past their realization date.** The objective is to provide an indicator of the effectiveness to handle risks in a timely manner.

4.10.7 References

1. U.S. Air Force, Air Force Materiel Command. *Risk Management*. Pamphlet 63101. AFMC, 09 July 1997.
http://www.sm.nps.navy.mil/mn3331_core/Calendar/Week6/Readings6/Risk_Mgt/US_AF_Risk_Mgmt_Guide.doc
2. American National Standards Institute/Electronic Industries Alliance. *Processes for Engineering a System*. ANSI/EIA-632-1998, pp. 11, 13, 14, 17, 30, 33-4, 45, 49, 52, 67, 75, 77, 81, 96, 109. Requirement 24.
3. Blanchard, Benjamin S., and Walter J. Fabrycky. *Systems Engineering and Analysis*. Third edition. Englewood Cliffs, NJ: Prentice Hall, 1998, pp. 657-661.
4. Conrow, Edmund H. *Effective Risk Management*. Reston, VA: American Institute of Aeronautics and Astronautics, Inc., 2000. <http://www.risk-services.com/aiaabok1.htm>
5. Department of Defense. *Transition from Development to Production*. DOD 4245.7-M. Chapter 9-8. Washington, DC: U.S. Department of Defense, September 1985.
6. U.S. Department of Transportation. *Departmental Guide to Risk Management Planning*. DOT H 1350.252. Washington, DC: U.S. Department of Transportation, 22 May 1999.

7. Defense Acquisition University Press. *Risk Management Guide for DoD Acquisitions*. Fifth edition. Fort Belvoir, VA: Defense Acquisition University Press, June 2002. http://www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm
8. Defense Systems Management College. *Systems Engineering Management Guide*. Chapter 15. Fort Belvoir, VA: Defense Systems Management College, 1990.
9. Electronics Industries Alliance. *Processes for Engineering a System*. EIA 632. Arlington, VA: Electronics Industries Alliance, January 1999. 08/09/02. Rev. 99, Chg.H. <http://www.eia.org>
10. Federal Aviation Administration. *FAA Acquisition Management System*. Paragraph 2.9.14. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration. <http://fast.faa.gov/>
11. Federal Aviation Administration. *FAA Acquisition Program Baseline Template*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration. <http://fast.faa.gov>.
12. Federal Aviation Administration. *FAA Orders 1900.47, 1050, 1600, 3900, and 1370.82*. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration.
13. Federal Aviation Administration. *Acquisition and Program Risk Management Guidance*. FAA P1810. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, December 1996.
14. Federal Aviation Administration. *Risk Assessment Guidelines for the Investment Analysis Process*. FAA Working Paper No. WP-59-FA7N1-97-2. Washington, DC: U.S. Department of Transportation, Federal Aviation Administration, July 1999.
15. Accounting and Information Management Division. *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making*. GAO/AIMD-10.1.13. Washington, DC: U.S. General Accounting Office, Accounting and Information Management Division, February 1997, Section 10.1.13.
16. Accounting and Information Management Division. *Information Security Risk Assessment*. GAO/AIMD-99-139. Washington, DC: U.S. General Accounting Office, Accounting and Information Management Division, August 1999.
17. U.S. General Accounting Office. *Determining Performance and Accountability Challenges and High Risks, Exposure*. Draft. GAO/OCG-00-12. Washington, DC: U.S. General Accounting Office, August 2000.
18. Grady, Jeffery O. *Systems Requirements Analysis*. New York, NY: McGraw-Hill, 1993, pp. 462-465. <http://www.mcgraw-hill.com/>
19. Grady, Jeffery O. *System Engineering Planning and Enterprise Identity*. Boca Raton, FL: CRC Press, 1995, pp. 168-177.
20. Grady, Jeffery O. *System Integration*. Boca Raton, FL: CC Press, 1994, p. 149.
21. Shish, Robert. *NASA Systems Engineering Handbook*. NASA SP-6105. Washington, DC: National Aeronautics and Space Administration, June 1995, pp. 37-44.
22. Office of Management and Budget. *Planning, Budgeting, Acquisition, and Management of Capital Assets*. OMB Circular No A-11, Part 7. Washington, DC: Office of Management and Budget, June 2006.

23. Project Management Institute. *A Guide to the Project Management Body of Knowledge* (PMBOK® Guide 2000 Edition). Chapter 11. Newton Square, Pennsylvania.
24. Ross, John F. *Living Dangerously: Navigating the Risks of Everyday Life*. Cambridge, MA: Perseus Publishing, 1999.
<http://www.questia.com/PM.qst?action=openPageViewer&docId=85921102>.
25. *Best Practices: How to Avoid Surprises in the World's Most Complicated Technical Process —The Transition from Development to Production*. DON NAVSO P-6071, March 1986.
26. Forsberg, Kevin, Mooz, Harold, and Cotterman, Howard. *Visualizing Project Management: Models and Frameworks For Mastering Complex Systems*. Hoboken, NJ: John Wiley & Sons, Inc., 2005. 3rd Edition, pp. 223-253
27. International Council on Systems Engineering (INCOSE). *Systems Engineering Handbook: A "What To" Guide For All SE Practitioners*. INCOSE-TP-2003-002-03, Version 3
28. Navstar GPS Joint Program Office (JPO) - HQ Air Force Space Command (AFSPC). *Risk Management Operating Instruction*. GP Operating Instruction 63-1108 (Rev 1 Draft), xx Nov 2005.